PRIME Privacy and Identity Management for Europe

Contract N° 507591

Title:	*Framework V3*
Author:	*WP 14.1*
Editor:	*Simone Fischer-Hübner, Hans Hedbom (Karlstad University)*
Reviewers:	*Marit Hansen (ICPP)*
	Peter Keller (Swisscom)
Identifier:	*D14.1.c*
Type:	*Deliverable*
Version:	*1*
Date:	*17 March 2008*
Status:	*Final*
Class:	*Public*

Summary

This document presents the holistic Framework for the PRIME project. It presents definitions for PRIME concepts and terminology and defines the Problem Space by describing trends in the processing of personal data from the technological, legal, business and societal perspectives, as well as the consequences of increased personal data use for the individual and society.
After presenting the vision of the PRIME project as shared by the project partners, it defines the prerequisites for the PRIME solution in form of aligned legal, social and economic requirements. Then it describes the PRIME solution by introducing a privacy management framework including a life cycle model for the development of online services. The life cycle model focuses on the decisions the developers have to make in producing privacy-enhanced processes, and on the core processes — data and meta data management —, in more detail. The implementation of these processes by means of PRIME components is discussed. Throughout the life cycle relevant socio-legal-economic aspects are highlighted. The client side is described by introducing client side processes and their implementation by means of PRIME components with a special focus on the role of the user interface. Besides, it is described how the PRIME solution can be integrated into applications. Finally other identity management solutions and initiatives are presented and compared with PRIME.

The PRIME project receives research funding from the Community's Sixth Framework Programme and the Swiss Federal Office for Education and Science.

Members of the PRIME consortium:

International Business Machines of Belgium	Belgium
IBM Zürich Research Laboratory	Switzerland
Unabhängiges Landeszentrum für Datenschutz	Germany
Technische Universität Dresden	Germany
Deutsche Lufthansa AG	Germany
Katholieke Universiteit Leuven	Belgium
T-Mobile International	Germany
Hewlett-Packard Ltd.	United Kingdom
Karlstads Universitet	Sweden
Università degli Studi di Milano	Italy
Joint Research Centre	Italy
Centre National de la Recherche Scientifique	France
Johann Wolfgang Goethe-Universität Frankfurt am Main	Germany
Chaum LLC	United States of America
Rheinisch-Westfälische Technische Hochschule Aachen	Germany
Institut EURECOM	France
Erasmus Universiteit Rotterdam	The Netherlands
Universiteit van Tilburg	The Netherlands
Fondazione Centro San Raffaele del Monte Tabor	Italy
Swisscom AG	Switzerland

Published PRIME documents

These documents are all available from the project website located at **http://www.prime-project.eu**

Excerpt of project "Description of work"	03-2004
Project presentation	09-2004
Overview of existing assurance methods	09-2004
Evaluation of early prototypes	12-2004
HCI guidance and proposals	02-2005
Framework Version 1	03-2005
Requirements Version 1	05-2005
White Paper Version 1	07-2005
Tutorials Version 1	06-2005
Architecture Version 1	08-2005
White Paper Version 1	07-2005
Evaluation of integrated prototype Version 1	07-2005
Initial application prototypes	12-2005
Evaluation of initial application prototypes	03-2006
General Public Tutorial	03-2006
Framework Version 2	07-2006
Architecture Version 2	12-2006
Advanced Tutorial Version 2	02-2007
Integrated Prototype Version 2	03-2007
Annual research report III	04-2007
User-side IDM integrated prototype V2	04-2007
White Paper Version 2	05-2007
Evaluation of Integrated prototype Version 2	05-2007
Final Application Prototypes	10-2007

The PRIME Deliverable Series

Vision and Objectives of PRIME

Information technologies are becoming pervasive and powerful to the point that the privacy of citizens is now at risk. In the Information Society, individuals need to be able to keep their autonomy and to retain control over their personal information, irrespective of their activities. The widening gap between this vision and current practices on electronic information networks undermines individuals' trust and threatens critical domains like mobility, healthcare, and the exercise of democracy. The goal of PRIME is to close this gap.

PRIME develops the PRIME Framework to integrate all technical and non-technical aspects of privacy-enhancing identity management and to show how privacy-enhancing technologies can indeed close this gap. PRIME elicits the detailed requirements from legal, social, economic, and application points of view and shows how they can be addressed. PRIME will enable the users to effectively control their private sphere thanks to the PRIME Architecture that orchestrates the different privacy-enhancing technologies, including the human-computer interface. To validate its results, PRIME develops prototypes and conducts experiments with end-users in specific application areas.

PRIME advances the state of the art far beyond the objectives of the existing initiatives to address foundational technology, through PRIME research on human-computer interface, ontologies, authorisation and cryptology, anonymous communications, and privacy-enhancing identity management systems architecture and assurance methods, taking into account legacy and emerging systems.

PRIME raises awareness of privacy-enhancing identity management through its white paper and tutorials, as well as press releases, leaflets, slide presentations, and scientific publications. The following PRIME materials are available from http://www.prime-project.eu

Introduction to PRIME

- Press releases, leaflets, and slide presentations outline the project objectives, approach, and expected results;
- The PRIME White Paper introduces privacy-enhancing identity management issues and PRIME's vision, solutions, and strategy;
- Tutorials introduce major concepts of privacy-enhancing identity management for use by the software development community and the general public.

PRIME technical materials

- PRIME Framework reviews privacy-enhancing identity management issues, PRIME legal, social, and economic requirements, PRIME concepts and models, and PRIME architecture outline;
- PRIME Requirements analyses in-depth the legal, social, economic, and application requirements. They comprise generic requirements, as well as specific, scenario-based requirements of selected application areas including eLearning, location-based services, and airport security controls.
- PRIME Architecture describes in-depth the organisation and orchestration of the different privacy-enhancing technologies in a coherent PRIME system;
- Annual research reports review the research results gained in PRIME over the past years, and the research agenda for the subsequent years;
- HCI Guidance provides a comprehensive analysis of the Human-Computer Interface requirements and solutions for privacy-enhancing identity management;
- Assurance methods surveys the existing assurance methods that are relevant to privacy-enhancing identity management;
- Evaluation of prototypes assesses the series of early PRIME technology prototypes from the legal, social, and economic standpoints;
- Scientific publications address all PRIME-related fields produced within the scope of the project.

PRIME work plan

PRIME global work plan provides an excerpt of the contract with the European Commission.

Foreword

PRIME Partners from various disciplines have contributed to this document. The following list names the main contributors for each chapter:

Chapter 1 (Introduction) was written by Simone Fischer-Hübner and Hans Hedbom;

Chapter 2 (Terminology) was updated by Marit Hansen and initially written by Giles Hogben with changes included by Christer Andersson, Simone Fischer-Hübner, and Ronald Leenes;

Chapter 3 (Problem Space) was jointly written by the following authors: Section 3.1 is based on section 3.1 in Framework V2 by Ronald Leenes, section 3.2 was written by Simone Fischer-Hübner and Hans Hedbom, section 3.3 by Eleni Kosta, section 3.4 by Alea Fairchild and Piet Ribbers including section 3.4.2 by Peter Keller, section 3.5 by Bart Priem and Isabelle Oomen, and section 3.6 by Simone Fischer-Hübner with input from Framework V2 by Ronald Leenes;

Chapter 4 (Vision of PRIME) was written by Simone Fischer-Hübner;

Chapter 5 (Solution) was jointly written by the following authors: section 5.1 by Simone Fischer-Hübner, section 5.2 by Eleni Kosta, Aleksandra Kuczerawy, Bart Priem and Alea Fairchild, section 5.3 by Alea Fairchild and section 5.4 is based on section 5.2 of Framework V2 written by Ronald Leenes, Jimmy Tseng, Dieter Sommer, Albin Zuccato, John Sören Pettersson and Simone Fischer-Hübner and was updated by Dieter Sommer, Alea Fairchild, John Sören Pettersson, Hans Hedbom and Simone Fischer-Hübner;

Chapter 6 (Application Scenarios) was written by the following authors: Simone Fischer-Hübner wrote section 6.1 (eShopping). The LBS scenario is based on the Framework V1 LBS scenario written by Georg Kramer, Lothar Fritsch, Markulf Kohlweiss, Christer Andersson and Simone Fischer-Hübner, and includes updates by Jan Zibuschka, Hans Hedbom and Simone Fischer-Hübner;

Chapter 7 (The Landscape of Identity Management) was written by Marco Casassa-Mont and Dieter Sommer;

Chapter 7 (Conclusions) was written by Simone Fischer-Hübner.

Table of Contents

Table of illustrations

List of acronyms

APIS	Advance Passenger Information System
CC	Creative Commons
CEN	Comité Européen de Normalisation
CEN DPP	CEN Data Protection and Privacy
CEN/ISSS	CEN Information Society Standardization System
CMBA	Creative and Media Business Alliance
CMMi	Capability Maturity Model Integration
DADA	Drag and Drop Agreement
DNA	deoxyribonucleic acid
DRM	Digital Rights Management
DVD	Digital Versatile Disk
CRM	Customer Relationship Management
DPA	Data Protection Authority
EC	European Commission
ECHR	European Convention on Human Rights
EDPS	European Data Protection Supervisor
EPC	Electronic Product Code
EU	European Union
FIM	Federated Identity Management
GPL	General Public License
GPS	Global Positioning System
GSM	Global System for Mobile Communication
HCI	Human-Computer Interaction
HTTP	Hypertext Transport Protocol
ICPP	Independent Centre for Privacy Protection
ICT	Information and Communication Technology
ID	Identity
IDM	Identity Management
IdP	Identity Provider
IMS	Identity Management System
IOI	Items of Interest
IP	Internet Protocol
ITIL	IT Infrastructure Library
iTMS	iTunes Music Store
ISO/IEC JTC	International Standards Organisation/International Electrotechnical Commission Joint Technical Committee
IST	Information Society Technologies
ISTPA	International Security Trust and Privacy Alliance
LBS	Location Based Service
MMORPG	Massively Multiplayer Online Role Playing Game
MRZ	Machine Readable Zone
MSN	Microsoft Network
MUD	Multi User Dungeon
NWI	New Work Item

NYSE	New York Stock Exchange
OASIS	Organization for the Advancement of Structured Information Standards
OECD	Organisation for Economic Co-operation and Development
P2P	Peer to peer network
PE-IMS	Privacy Enhancing Identity Management System
PET	Privacy-Enhancing Technology
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
PRIME	Privacy and Identity Management for Europe
RFID	Radio Frequency Identification
SET	Secure Electronic Transaction
SLE	Social, Legal, and Economic
SNG	Studio Notarile Genghini
SWOT	Strengths, Weaknesses, Opportunities and Costs
TDQM	Total Data Quality Management
TPM	Trusted Platform Module
UI	User Interface
US	United States of America

1 Introduction

1.1 Aims and Scope

This document establishes the Framework V3 for the PRIME project.

A framework can be defined as a skeletal, structural frame [142] which provides a particular set of rules, ideas, or beliefs which are used to deal with problems or to decide what to do [22].

The PRIME Framework is a holistic framework for privacy-enhancing identity management defining the PRIME concepts and terminology, problem space and objectives, the vision of the project, and the PRIME solution and a selection of applications. The PRIME Framework integrates technical and non-technical aspects and research results that are elaborated by partners from various disciplines within the PRIME project. It has served as a forum to facilitate interdisciplinary exchange between PRIME partners. Besides, it should also serve as a reference for all concerned stakeholders and thereby provides the basis for the widespread deployment of privacy-enhancing mechanisms and identity management.

1.2 Related work

There are other PRIME deliverables, such as the Requirements and Architecture deliverables and the PRIME book, that also document main project results. However, the PRIME Architecture and Requirements deliverables provide more detailed information and focus on the technical components, whereas the Framework deliverables should provide a more abstract view, integrating non technical and technical components on a level that is understandable by partners from various disciplines and concerned stakeholders. In the PRIME book, all involved disciplines will present in depth their research results in various chapters, whereas the Framework summarises main project results and provides a more integrated view on the results from the involved disciplines.

The Framework expands concepts outlined by the PRIME White Paper. The PRIME White Paper is targeted to the outside world and has a higher level of abstraction than the Framework document. The Framework deliverables have been addressing the PRIME stakeholders as well as the participants in the project.

Related work outside the PRIME project includes the following frameworks and white papers:

The Open Group White Paper on Identity Management [123] explores technical key concepts of identity management (IDM) and examines identity management from various perspectives, including business, security, personal, and technical. A support for strong privacy is, however, not covered.

The Liberty Alliance also has issued white papers, including one on Personal Identity [79]. These are, however, in comparison to the PRIME Framework on a high level of abstraction primarily focusing on technical Identity Management and related security issues, such as technical aspects of user control, federated identity management (FIM), identity-based web services and identity theft protection.

Also Microsoft has published white papers on “Microsoft’s Vision for an Identity Metasystem” [91] and “The Laws of Identity” [13] outlining the technical design principles and architecture of their CardSpace system. These white papers are focusing on technical issues of an Identity Metasystem on a high abstraction level. Guiding privacy principles “User Control and Consent” and “Minimal Disclosure for a Constrained Use” for their Identity Metasystem correspond to some of the PRIME technical design principles, but are not elaborated in much detail.

The “Identity Management Systems: Identification and Comparison Study” [64] by PRIME partner ICPP and SNG also presents a multidisciplinary framework for privacy-enhanced identity management (IDM), which includes technical, legal and sociological perspectives for the definition of terms and presents usage scenarios. However, a major focus of the ICPP/SNG comparison study is the analysis of available identity management applications and a survey on expectations with regard to identity management systems. In comparison to the ICPP/SNG study, the PRIME Framework addresses also the business perspective and presents a holistic PRIME solution including a technical architecture (PRIME architecture).

ISTPA (International Security, Trust & Privacy Alliance) [66] has issued a Privacy Framework that aims at providing an analytical starting point and basis for developing products and services that support privacy regulations. It is however focusing on US privacy principles and fair information practices as defined by the U.S. Federal Trade Commission, which provide a weaker protection than the European Legal and Regulatory Privacy Framework.

ISO/IEC JTC 1/SC 27 is working on a "Framework for Identity Management" and has currently also two related study periods running, one on Identity Management, and one on Privacy. Back in 2004 the first proposal for a New Work Item (NWI) on a framework for identity management, that ISO/IEC JTC 1/SC 27 got (from the US), had a focus on technical security concepts, especially role-based access control, i.e. it only provided a particular technical perspective and the emphasis was not on strong privacy protection. This has changed with the final set-up of the NWI that was created in April 2005 and with the first draft of the framework. The draft has undergone several iterations; however, it is not complete yet. The scope of the standard is to define concepts and processes of managing identity information on a high level. Moreover a working draft on a privacy framework and one on a privacy reference architecture is under development. However, at this stage it is too early to say exactly what the privacy framework will comprise. The aim is to define a framework for defining privacy safeguarding requirements as they relate to personally identifiable information (PII) in any jurisdiction. Further the study period on Privacy in SC 27 is starting initiatives to standardize among other things Entity Authentication Assurance, and Access Management. SC 27/WG 5 is also starting two new internal study periods on Access Control Mechanisms and Privacy Capability Maturity Models.

ITU-T SG 17 has established a Focus Group on Identity Management. The group is working on a report on an Identity Management Framework for Global Interoperability and have among other things performed a gap analysis on identity management uses cases and keeps what they call a "living list" on terms and definitions in relation to identity management. The work in this group is primarily focused on high level requirements for the interoperation between different types of identity management systems and has so far mainly focused on technical aspects of interoperability.

1.3 Changes to Frameworks V0, V1 and V2

In comparison to the earlier versions V0 and V1 of the PRIME Framework, Framework V2 has applied a more integrated approach to present the various non-technical and technical aspects of the problem space, the PRIME solution and one selected application scenario.

Framework V3 is building upon Framework V2, but includes several important changes and updates. In particular, the terms and definitions have updated and aligned to the recent version of the terminology paper by Pfitzmann and Hansen [102]. Besides, the sections in the problem space chapter on legal, social and economic developments have been more or less rewritten taking recent developments into account. Before presenting the PRIME solution, the prerequisites for achieving it are elaborated in form of an integrated overview on PRIME's legal, social, economic requirements, which tries to put these requirements into relation. Besides, an Identity and Access Management Maturity Model with PET Extensions is briefly presented in this context. Also the PRIME solution in form of the Privacy Management Framework has been updated by integrating the latest project results from the PRIME Architecture, HCI and Economic Requirements work packages. Besides, Framework V3 is now demonstrating how PRIME can be integrated into applications for the privacy-sensitive application areas of eShopping and Location-Based Services (LBS). These application scenarios illustrate PRIME's core ideas in a practical context. Another major contribution is a new chapter on the Landscape of Identity Management, which positions PRIME in relation to other Identity Management initiatives.

1.4 Structure of this Deliverable

The remainder of this document is structured as follows:

Chapter 2 (Terms and Definitions) presents definitions for PRIME concepts and terminology.

Chapter 3 (Problem Space) defines the Problem Space: It describes trends in the processing of personal data from the technological, legal, business and societal perspectives, as well as the consequences of

increased personal data use for the individual and society. Besides, it shows why current solutions fall short and in what respect PRIME can help.

Chapter 4 (Vision) summarises the vision of the PRIME project as shared by the project partners including the PRIME design principles as a core part.

Chapter 5 (Towards the PRIME Solution) defines first the prerequisites for the PRIME solution in form of aligned legal, social and economic requirements. Then it describes the solution by introducing a privacy management framework including a life cycle model for the development of "online" services, and by describing the client side of the interaction between user and online service with a special focus on the role of the user interface.

Chapter 6 (Application Scenarios) illustrates how the PRIME solution can be applied in the areas of eShopping and Location Based Services.

Chapter 7 (The Landscape of Identity Management) describes other Identity Management initiatives and compares PRIME with them.

Finally, chapter 8 (Conclusions) provides final conclusions.

2 Terms and Definitions

As PRIME has integrated partners from many disciplines, it has been vital that the participants could agree on a common terminology to be used throughout the project. This has facilitated discussion among researchers and influenced the priorities and directions of research. It has also constituted a basis for the formal ontology used within the PRIME applications. This chapter describes the core set of concepts relevant for privacy and Identity Management (IDM). An editor with expert knowledge in the area was assigned to define each term. Comments from many PRIME researchers were integrated over a period of several months in order to reach consensus on these definitions within the consortium. Many of the definitions are based on [102].

- **Anonymity:** Anonymity of a subject from an adversary's perspective means that the adversary cannot sufficiently identify the subject within a set of subjects, the anonymity set.
- **Anonymity Set:** The set of all possible subjects in a given data collection context.
- **Certificate:** A digitally signed statement which authenticates the public key as belonging to the holder of a given pseudonym or civil identity. Can include period of validity.
- **Credential:** Evidence or testimonials concerning authorizations to actions or reputation made by one entity (issuer) about another entity (user).
- **Anonymous Credential:** Anonymous credentials (also called private or convertible credentials) are secondary credentials that are derived from a certificate issued on a different pseudonym of the same person. Multiple anonymous certificates can be created from a single certificate that are neither linkable to each other nor to the issuance interaction in which the master certificate was obtained.
- **Claim:** A claim is a statement made by an entity (the claimant) about another entity (the claim's object) to an entity or set of entities (the claimant's addressee). A claim can be endorsed by a third party, which certifies the claim in an integrity-protected manner. An example for a claim is "The requester is of age greater than 18 years, claimed by the requester, endorsed by an EU-member-state-issued passport"). A *claim request (or: request for claims)* is issued in order to obtain claims that satisfy the access control policy for a requested resource.
- **Data Subject:** A person who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to her physical, physiological, mental, economic, cultural or social identity (see Art. 2.a EU Directive 95/46/EC).
- **Data Controller:** The entity (e.g. legal or natural person or other body) defined to be responsible for processing of personal data processing according to national or Community laws or regulations (see Art. 2.d EU Directive 95/46/EC).
- **Identical:** Having all possible properties in common.
- **Identifiability:** Identifiability of a subject from an adversary's perspective means that the adversary can sufficiently identify the subject within a set of subjects, the identifiability set.
- **Identifier:** A symbol or a set of symbols of a subject which refers to a concept allowing to distinguish it from others in a specific scope. This could be a name which is imposed by a third party.
- **Identity:** A symbol or a set of symbols referring to an entity, i.e. a subject or an object, allowing to distinguish it from others in a specific scope. The identifier could be a name which is imposed by a third party, being unique in a specific namespace.
    - **Civil Identity:** Identity attributed to a person by a State (e.g. represented by the social security number or the combination of name, date of birth, and location of birth etc.).
    - **Digital Identity:** Attribution of attributes to a person, which are immediately operationally accessible by technical means. Digital identity should denote all those

personally related data that can be stored and automatically interlinked by a computer-based application.

- **Identity Management:** Identity management means managing various partial identities (usually denoted by pseudonyms) of a person, i.e. administration of identity attributes including the development and choice of the partial identity and pseudonym to be (re-)used in a specific context or role.
- **Identity Management System (IMS):** An identity management system in its broadest sense refers to technology-based administration of identity attributes including the development and choice of the partial identity and pseudonym to be (re-)used in a specific context or role.
- **Partial Identity:** Any subset of attributes of a complete identity, which characterises a person to some degree within an anonymity set. Partial identities usually represent the person in a specific context or role.
- **Privacy-Enhancing Identity Management:** Given the restrictions of a set of applications, identity management is called privacy-enhancing if it sufficiently preserves unlinkability (as seen by an adversary) between the partial identities of a person required by the applications. Identity management is called perfectly privacy-enhancing if if it perfectly preserves unlinkability between the partial identities, i.e. by choosing the pseudonyms (and their authorizations) denoting the partial identities carefully, it maintains unlinkability between these partial identities towards an adversary to the same degree as giving the adversary the attributes with all pseudonyms omitted.
- **Privacy-Enhancing Identity Management System (PE-IMS):** A Privacy-Enhancing IMS is an IMS that, given the restrictions of a set of applications, sufficiently preserves unlinkability (as seen by an adversary) between the partial identities and corresponding pseudonyms of a person.
- **User-Controlled Identity Management System:** A user-controlled identity management system is an IMS that makes the flow of the user's identity attributes explicit and gives its user a large degree of control. The guiding principle is "notice and choice".
- **Virtual Identity:** Sometimes used in the same meaning as digital identity or digital partial identity, but because of the connotation with "unreal, non-existent, seeming" the term is mainly applied to characters in a MUD (Multi User Dungeon), MMORPG (Massively Multiplayer Online Role Playing Games) or to avatars.

- **Informational Privacy:** Self-determination of what information is known about a person and how it is used.
- **Spatial Privacy:** The individual's control of what information is presented to their senses.
- **Linkability:** Linkability of two or more items of interest (IOIs, e.g. subjects, messages, actions, …) from an adversary's perspective mans that within the system (comprising these and possibly other items), the adversary can sufficiently distinguish whether these IOIs are related or not.
- **Personal Data:** Any information relating to an identified or identifiable natural person, the "data subject" (see Art. 2.a EU Directive 95/46/EC).
- **Pseudonym:** A pseudonym is an identifier of a subject other than the subject's civil identity.
  - **Person Pseudonym:** A substitute or alias for a data subject's civil identity (name) which may be used in many different contexts.
  - **Relationship Pseudonym:** A pseudonym that is used in regard to a specific communication partner (e.g. distinct nicknames for different communication partners).
  - **Role Pseudonym:** A pseudonym that is chosen for the use in a specific role (e.g. patient or customer).

  - **Role-Relationship Pseudonym:** A pseudonym that is used for a specific combination of a role and communication partner.
  - **Transaction Pseudonym:** A pseudonym that is used for a specific transaction only, i.e. for each transaction, a different pseudonym is used.

- **Pseudonymity:** Pseudonymity is the use of pseudonyms as identifiers.
- **Sensitive Data**:
  - A special category of personal data which individuals on average prefer to be known only to a few selected others and thus merits special legal protection (see Art. 8 EU Directive 95/46/EC: "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life").
  - From an individual's perspective those personal data which the individual prefers to be known only to a few selected others.
- **Undetectability:** Undetectability of an item of interest (IOI) from an adversary's perspective means that the adversary cannot sufficiently distinguish whether it exists or not:
- **Unlinkability:** Unlinkability of two or more items of interest (IOIs e.g., subjects, messages, actions, etc.) from an adversary's perspective means that within the system (comprising these and possibly other items), the adversary cannot sufficiently distinguish whether these IOIs are related or not.
- **Unobservability:** Unobservability of an item of interest (IOI) means
  - Undetectability of the IOI against all subjects uninvolved in it and
  - Anonymity of the subject(s) involved in the IOI even against the other subject(s) involved in that IOI.

3 Problem Space

3.1 Introduction

We move from a paper based world into a network based society, the consequences of which are not fully understood. Paper based processes are being replaced by electronic processes that superficially resemble them. Email, for instance, appears to be traditional mail on steroids. But on closer inspection it has (radically) different characteristics: sender, recipient, subject, and content can be inspected by more people than was the case with traditional mail, while some of the traces created during transmission persist after delivery[1]. From a privacy perspective this difference matters. Also completely novel processes and applications emerge that often affect privacy in ways not clear to the user. Instant messaging such as MSN, for instance, did not exist prior to the internet. These services appear to be anonymous because they allow users to adopt pseudonyms or nicknames. In reality, the use of these applications leaves traces all the time. Traces that often can ultimately identify users. But even when this is not the case, they can be used for profiling and data mining thereby still affecting the users.

The meaning of privacy changes due to the introduction of information and communication technologies (ICTs) in daily life. Privacy primarily related to spatial privacy, such as protection one's home from intrusion by the state. Informational privacy is nowadays gaining importance urging us to also think about our identity and even manage it. In the offline world, deciding what personal data to disclose to others is relatively fluid; we give away more details of ourselves as the need arises. In the online world identity management increasingly becomes an issue to think about. This also applies to service providers. They have to decide how to treat (returning) customers. Customer data is an asset and hence thinking about what one wants to know about a customer is important.

In the following sections we discuss some developments in four spheres: technological advances, business, legal, and societal developments to show the complexities of the use of PII in the advancing society and to understand the problems the PRIME project seeks to address.

3.2 Technical Developments

Technological advances allow the delivery of new kinds of services. ICTs are technologies of control [70]. They have a strong tendency to undermine privacy and to limit the individuals' control over their personal spheres. They produce data, either intended, or as a side effect of their primary function. Every click on a website produces IP numbers of origin and destination — traffic data —, which are necessary to produce the page in the user's browser. These data reveal information about the user and her interests, especially if they include information about the content of the interaction (e.g., a Google search term). The data allows for consumer profiles to be constructed to offer tailor made services, but also to exclude users from services. They can also be used for surveillance purposes. Apart from this secondary kind of dataveillance[2], also more pervasive tracking techniques such as cookies, web bugs and spyware exist to secretly monitor online users and their browsing habits.

Personal data, which has always been an important corporate and strategic asset for companies and governments, can now be effectively analysed and explored with modern data mining techniques for discovering patterns and correlations in databases. Such discovered patterns allow to classify individuals into categories and are thereby revealing confidential personal data with a certain probability. The results can be used for bahavioural targeting, specifically addressing an individual with offers or advertisements on the basis of these profiles, and social sorting, i.e. making decisions on the basis of social characteristics of an individual such as ethnical, sexual or social group (e.g., [87]). Besides, with the help of inductive

[1] See section 3.3.2

[2] Dataveillance is the combination of Data and Surveillance: '... the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons.' [20]

learning techniques, data mining tools may disclose confidential and sensitive facts and predict confidential attributes about individuals (e.g., customer buying power or medical diagnosis).

Data sharing across government agencies and with the private sector, which has increasingly been proposed and practiced after 9/11, in combination with data mining allow the creation of new profiles or expand existing profiles of individuals. There are, for instance, proposals for a next generation computer-assisted passenger prescreening system that will use data from credit-reporting agencies and other companies, and even previous flights and registries, for data mining (see [120]).

Biometric identification technologies, or in short biometrics, are at the brink of wide-spread deployment, for instance in the biometric passports that should be fully implemented throughout the EU member states by the end of 2007. Biometric identification technology refers to the automatic recognition of individuals based on their physiological and/or behavioural characteristics. Examples of biometric identification schemes include face recognition, iris or retina scan, fingerprint recognition, key stroke dynamics, and DNA identification. Although biometrics can be used as a privacy tool to unambiguously associate some credential to an individual e.g., the presenter of this card, identified by her fingerprint, is over 18 years of age, the common use is of a privacy threatening kind. Biometrics are used for verification/authentication of a person's identity. The biometric passport reveals the identity of the person showing the passport with embedded biometric features. It may even be used for direct identification in the case of centralized biometric databases as planned in various EU countries. Privacy concerns arise because Biometric samples collected for identification purposes can usually be used to derive further sensitive information. For instance, research gives evidence that from the raw picture of the iris certain diseases, such as glaucoma and iritis, can be diagnosed and genetic fingerprints (DNA) taken for forensic purposes can also be used to reveal parantage, gender and with some likelihood ethnicity [54].

Besides, biometric identification is threatening to take away the veil of anonymity of many daily transactions as they can serve as unique personal identifiers and allow to create an electronic trail of individuals' movements and habits. For instance, face recognition based on computerized pattern matching technology to automatically identify people's faces is increasingly used in combination with video surveillance at airports and public events, and thus enables the secret identification and classification of people in public. The trend of wide-range implementation and use of biometrics in passports and for border controls leads to massive data collection and storage. It creates a highly complex infrastructure that allows for the unrestrained monitoring and profiling of individuals.

Location based services (LBS) and context-aware services are another type of emerging technology that has profound effects on privacy. They may offer many useful and popular services, such as travel navigation, friend finder, and mobile dating. They require the processing of the geographical locations of the user, which might reveal sensitive personal details. Location data in combination with the user's preferences, business activities and the kind of information that a user requested, could be compiled and stored by service providers in detailed user profiles. Push LBS applications where information is automatically "pushed" to the user by the LBS provider at regular intervals (as used for mobile marketing or mobile disaster management LBS applications, for instance) often require user profiling to some extent in order to provide adequate information. These data can of course be used for other purposes as well such as unwanted marketing (SPAM), digging in the past, and blackmailing.

Information about social interactions, which is often of a private nature, can also be misused. This is especially an issue for multi-user LBS scenarios (used in peer-to-peer applications, e.g., friend finder, mobile dating). But social information can also easily be inferred from normal use. Network operators and service providers that have access to location data of different mobile users can easily compare the location profiles of two mobile users and derive information about the users' co-location. This could reveal information about when, and for what length of time, two users have spent time, or possibly been travelling together [51]. Hence, location data for single-user LBS, and even location information as part of traffic data, can also reveal information about social networks.

Location data can also be misused for unsolicited real time location tracking by using the information about the movements of mobile users. If the location information is not properly protected, people can

be tracked for the purpose of robbery, kidnapping or looting. These problems intensify if service providers and/or network operators link up their data sources.[3]

One of the biggest challenges for privacy for the future is posed by the advance of ubiquitous computing, where computers are seamlessly integrated in the environment and (personal) data processing becomes increasingly invisible for the individuals. Users will generally not see what data is being processed, by whom, and for what purpose. This further decreases their possibilities to control the disclosure of their personal data.

A form of ubiquitous technology that is already in use today is RFID (Radio Frequency Identification) technology. It is in use for a number of application areas such as medical applications (for preventing counterfeiting of drugs, and for tracking medical personnel in the hospital), security and access controls or supply chain applications. It potentially allows for the secret tracking of personal belongings, whereabouts and social networks. The unique item identification inherent in the proposed Electronic Product Code (EPC) standard for RFID tagging of items, for instance, could be used to profile individuals according to the items they are wearing or carrying. The EPC of commonly carried items, such as a person's watch, could also be used as personal identification code of this person, which would enable unprecedented new forms of surveillance (see also section 4.7). The uniqueness of these types of codes makes it very hard to judge if the information stored on the RFID tag is personal data or not since it is dependent on the type of item that is tagged and in what context the tag is read. In order to asses the "sensitivity" this type of information some form of lifecycle analysis of the data is needed.

In the more distant future, we may see sensor networks, which are developed for applications ranging from climate sensing, or monitoring factory instrumentation to tracking patient movements in hospitals. They are the key to the creation of so-called smart spaces, spaces that really react to their inhabitants. But also smart dust, a network of miniature wireless sensor nodes equipped with wireless communication facilities, are being developed. These networks can, due to the very small size of the individual nodes (hence the name 'dust') unobtrusively detect anything from light and temperature, to vibrations, etc. Sensor networks supplement traditional site surveillance methods but aggravate the privacy problem as they make large quantities of information easily available via remote access [17].

Technology, however, may not only limit the individual's privacy, it can also be used to protect privacy. Privacy Enhancing Technologies (PETs) are being developed specifically for this purpose, for instance in PRIME. PET developments will be further discussed in following chapters 4 and 5.

3.3 Legal Developments

3.3.1 Introduction

The main legal instruments that regulate the issue of processing of personal data in the European Union are the Data Protection Directive 1995/46/EC [35] and the ePrivacy Directive 2002/58/EC [36], which includes specific provisions regarding the processing of personal data in the electronic communications sector. The directives are being complemented by the Opinions of the Article 29 Working Party[4] and the European Data Protection Supervisor (EDPS), who examine practical issues and try to give guidance to the appliers of the law.

The need to enhance the level of law enforcement cooperation required to create the area of freedom, security and justice (cf. Art. 29 TUE), was first introduced in the Hague programme. Increase of such co-operation equals to an exchange of information between different authorities and consequently raises issues of protection of personal data. A multitude of legislative initiatives have been proposed – and more are in the pipeline- that relate to the processing of personal data in data exchanges between

[3] Recently the Art. 29 Working Party issued an opinion on the use of location data with a view to providing value-added services [5]).

[4] Under Article 29 of the Data Protection Directive, a Working Party on the Protection of Individuals with regard to the Processing of Personal Data is established, made up of the Data Protection Commissioners from the Member States together with a representative of the European Commission. The Working Party is independent and acts in an advisory capacity. The Working Party seeks to harmonize the application of data protection rules throughout the EU, and publishes opinions and recommendations on various data protection topics.

police and judicial authorities, the principles that such exchanges shall respect etc. Although the law-making activities related to issues of protection of personal data and privacy never ceases and covers a vast variety of sectors, we will focus in this chapter on the European initiatives that aim at regulating data protection issues in activities that were left outside from the protective ambit of the data protection directive. In view of the Reform treaty and the possible collapse of the pillar structure of the European Union, it will be very interesting to see how the diverging and topic-specific pieces of legislation will formulate a space of adequate protection of personal data. The provisions of the data retention directive relate also to the processing of personal data in the third pillar, as the retained data are going to be used by law enforcement authorities for the investigation and detection of serious crime. The directive is currently being transposed by the Member States and some implementation issues present great legal interest. Furthermore we will briefly analyse the proposal of the European Commission for the reform of the ePrivacy directive, in the frame of the reform of the European legal framework for electronic communications, and we will present the European initiatives on RFID technology, which is one of the hottest topics in the agenda today.

Of course, PRIME technology can not be presented as a direct solution to the problems that arise by the increased exchange of personal data and the call for more co-operation that involves exchanges of such data. Nevertheless, even if the PRIME identity management system will not be used as such, when processing of personal data takes place in the field of police and judicial co-operation, some core elements of the PRIME technology, such as the option to allow access to data only by some authorised entities, or the possibility given to the user to track their data, can be of great use.

The same is true for RFID-related privacy problems. Even though PRIME cannot solve them completely, a PRIME-based Identity management solution as presented in the PRIME Framework V1 can at least enhance privacy and control for users and thus be an important part of a holistic approach to privacy protection.

3.3.2 Legal Developments Regarding Data Protection in the Field of Law Enforcement

3.3.2.1 Draft Framework Decision on Data Protection in the Third Pillar

The data protection directive excludes in Article 3(2) al. 1 activities that clearly fall outside of Community law, such as the ones relating to a "common foreign and security policy"[134] or to "police and judicial cooperation in criminal matters"[135]. Although the processing of personal data carried out by police authorities is still not regulated at European level, it still falls under the protective ambit of Article 8 of the European Convention on Human Rights [26], which explicitly states that "there shall be no interference by a public authority with the exercise of [the right to respect for private and family life] except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others"[5], as well as the Convention 108 of the Council of Europe for the protection of individuals with regard to automatic processing of personal data. Furthermore data protection rules in the general frame of police and judicial co-operation regulate the processing of personal data in Schengen, Europol, Eurojust or the Customs Information System.

The processing of personal data in the field of police and judicial co-operation is absolutely necessary and unavoidable. Especially after the terrorist attacks in Madrid and in London, the interest in police cooperation throughout the European Union and its regulation in such a way in order to ensure greater efficiency has grown. Therefore the initiative of the European Commission in October 2005[6] to regulate the issue of protection of personal data processed in the framework of police and judicial co-operation in criminal matters was welcomed as a general idea. However the text of the Draft Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters (hereafter "draft framework decision on data protection in the third pillar") has been the apple of discord at European level and the proposal has still not been adopted

[5] Article 8 ECHR
[6] Proposal for a Draft Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters, COM (2005) 475 final, 04 October 2005

by the Council of the European Union. Ultimate goal of the draft framework decision is to achieve a balance between the two interests at stake, i.e. the protection of public order and the right of every individual to privacy [73]. As the European Data Protection Supervisor has pointed out, the data protection rules in police field should not only respond to "justified needs of law enforcement but should also protect the data subject against unjustified processing and access" [41]. Like the data protection directive made a balance between the free flow of information and the right to privacy of the data subject, a data protection framework in the third pillar shall ensure the effective police action without lowering the right of data subject in an unjustified and disproportionate way. This can become a very difficult task, taken into consideration the modalities of law enforcement. In any case any derogation from the general principles of data protection should be limited and well defined and restrictions shall be, where possible, partial and limited in time. [7]

An important issue the framework decision is dealing with is whether it should apply only to the exchange of personal data between law enforcement agencies of the different Member States or should cover every data processing in the law enforcement field.[8] Although the EDPS has advocated to the contrary, the latest version of the Framework Decision seems that it will probably limit its scope of application to the cross-border exchange of personal data. As a counterbalance to such limitation, an evaluation clause is planned to be introduced, compelling the European Commission to measure the level of implementation of the Draft Framework Decision four years after it becomes effective. Relevant to this is the issue of how the transmission will take place both between the police and judicial authorities within the European Union, as well as to or from authorities outside the European Union in the frame of international police co-operation.

Another important issue is whom the decision will cover, and mainly whether it will apply only to national authorities or it will also apply to Europol, Eurojust and the third-pillar Customs Information System. The initial proposal of the European Commission was excluding Europol, Eurojust and the third-pillar Customs Information System from the field of application of the decision. This approach has however been contested by the European Data Protection Supervisor, who rather sees it as "a good idea to harmonise their provisions, where necessary, and ensure the proper connections, consistencies and perhaps also some efficiencies." [63]. The same approach was also supported by the German Presidency of the Council.

The Working Party on Police and Justice, has expressed the opinion, along with the European Data Protection Supervisor and the European Data Protection Authorities, that "data protection principles should be adequately taken into account within the framework of fair co-operation also at EU level, in particular when attempting to develop and bring about a harmonised set of legal rules that are expected to regulate these matters for several years"[9]. Due to the special character of law enforcement, however, these principles can not be used as such in a new legal instrument for law enforcement in the third pillar. These rules have to be taken into consideration and serve as the basis for what will apply to the third pillar, taking into account the special needs of law enforcement.[10]

Ensuring the rights of the data subject is of paramount importance in the field of police and judicial cooperation in criminal matters. Furthermore the quality of the data processed in the course of police investigations is particularly sensitive, as a significant part of the information collected does not necessarily reflect the reality. Databases of investigatory and law enforcement bodies contain a multitude of information that is not regularly updated and data included in them can stem from testimonies or personal assessments of witnesses.

3.3.2.2 Draft Framework Decision on Availability

The Hague Programme considered the "principle of availability" as a new principle for the exchange of law enforcement information that would assist in the removal of the obstacles for the information needed for the fight against crime and terrorism to cross the internal borders of the European Union.

[7] As quoted by the Foundation for Information Policy Research, [53].
[8] For a detailed analysis on the topic see [73]
[9] Comments from the Working Party on Police and Justice with respect to the proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, http://www.statewatch.org/news/2007/nov/eu-dp-wppj-statement-on-dpfd.pdf
[10] For a detailed analysis of the privacy principles and the way they shall be applied in the third pillar, see [73]

The adoption of a legislative proposal that would cover the "principle of availability" was confirmed by the Council and Commission Action Plan implementing the Hague Programme, which was adopted by the Justice and Home Affairs Council of 2 and 3 June 2005, along with the presentation of a Proposal on adequate safeguards and effective legal remedies for the transfer of personal data for the purpose of police and judicial cooperation in criminal matters. In fact the Council of the European Union, during a meeting of the Justice and Home Affairs Council in an extraordinary session on the 13th of July 2005, asked the Commission to present the proposal on the principle of availability by October 2005. It should be pointed out that the introduced proposals go beyond the information exchange provided for by the Schengen Convention. The Framework Decision on the exchange of information under the principle of availability constitutes a new form of cooperation, which did not previously exist and it is therefore not part of the Schengen acquis introduced to the European Union by the Schengen Protocol.

The Explanatory Memorandum of the Proposal of the Council Framework Decision from the 12 October 2005[11] clarifies that the actual subject of the principle of availability is "the exchange of law enforcement information to uniform the conditions across the Union. If a law enforcement officer or Europol needs information to perform its lawful tasks, it may obtain this information, and the Member State that controls this information, is obliged to make it available for the stated purpose"[12]. The main innovation introduced by the Framework Decision is the direct online access to available information and to index data for the information that is not accessible online, for the Member States' law enforcement authorities and the Europol officers.

The Framework Decision emphasises direct channels of information exchange and includes a general obligation to reply, but with a limited number of harmonised grounds for refusal. The reason for that would be to speed the process and create more predictable outcome[13]. This point is presented as a strong advantage over the provision of Article 39 of the Convention Implementing the Schengen Agreement of 1990, which did not oblige the Member States to reply to a request for information, with severe implications for the individuals. At the same time other initiatives on similar matters have been presented at European level, such the proposal of the Kingdom of Sweden for a Draft Framework Decision on simplifying the exchange of information and intelligence[14], which seeks to improve the mechanism established by the Schengen Convention and harmonises the legal framework for the exchange of data and reducing response times. The principle of availability was already introduced in the Prüm Convention[15], also referred to as "Schengen III", which was initially signed by seven Member States.

3.3.2.3 Prüm Convention and its Embodiment in the European Legal System

The Prüm Convention on "the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration" was signed by Austria, Belgium, France, Germany, Luxembourg, the Netherlands and Spain on the 27th of May 2005. Although the scope of the Convention clearly falls in the field of police co-operation of the area of Freedom, Security and Justice of the EU and EC treaties [154] it was not adopted following the law making procedure within the European Union for legal instruments under the third pillar. It started as a multilateral agreement outside the European Union, just like the Schengen Convention, a reason why it is broadly known as "Schengen III". As the Prüm Convention serves the main goals laid down in the Hague Programme regarding the fight against crime and terrorism, an initiative of 15 European Member States[16] was launched, with a view to adopting a Council Decision on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime [17]. Such integration was presented as an

[11] COM (2005) 490 final
[12] Article 14 of the proposal
[13] Explanatory Memorandum
[14] 13986/4/05 REV 4
[15] Convention between the Kingdom of Belgium, the federal Republic of Germany, the Kingdom of Spain, the French Republic, the grand Duchy of Luxemburg, the Kingdom of the Netherlands and the Republic of Austria on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration, signed by the contracting parties in Prüm (Germany) on the 27 May 2005
[16] The Kingdom of Belgium, the Republic of Bulgaria, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands, the Republic of Austria, the Republic of Slovenia, the Slovak Republic, the Italian Republic, the Republic of Finland, the Portuguese Republic, Romania and the Kingdom of Sweden
[17] (2007/C 71/13), Official Journal of the European Union, C71/35, 28.03.2007

alternative to the draft decision on availability, as viewed by the EDPS[18], which has been – at least temporarily - put aside by the Council. The political agreement regarding the Prüm Convention has been greeted by Commissioner Frattini as "a very important first step in view of the implementation of the principle of availability"[19].

The Prüm Convention and the relevant Council Decision introduce far-reaching measures to improve information exchange. Some similarities, such as the index system and direct access to national databases can be found with the Framework Decision on data protection in the third pillar that was already presented under 3.3.2.2. The Prüm Convention aims at the improvement of the "exchange of information between the parties entering into the convention in order to enable this to take place in a simplified and more rapid manner"[20]. The Convention and the decision introduce specific means of cross-border cooperation, such as the exchange of information on DNA data, fingerprints and vehicle registration [73].

Further to his first Opinion on the initiative of the Council of the European Union to incorporate the Prüm Treaty into European legislation, the EDPS adopted an opinion on the 19th of December on the German initiative establishing implementing rules which are necessary for the functioning of the Council Prüm initiative [42]. The implementing rules that are proposed by the EDPS are of great importance when exchanges of data take place. The EDPS recommends that the combination of general provisions and specific tailored rules on data protection should ensure both the rights of citizens and the efficiency of law enforcement authorities when the proposal enters into force. Furthermore the accuracy in searches and comparisons of DNA profiles and fingerprints should be duly taken into account and constantly monitored and the relevant data protection authorities should be put in a position to properly carry out their supervisory and advisory role throughout all the different stages of the implementation.

3.3.3 Data Retention Directive

3.3.3.1 Introduction to the Directive

The data retention directive [37] was adopted on the 15th of March 2006. The directive applies to providers of publicly available electronic communications services or of public electronic communications networks and it aims at harmonising the obligations of these providers with regard to the retention of traffic and location data, as well as the data necessary to identify subscribers or registered users, to ensure that these data are available for law enforcement purposes. Information to be retained is the information relating to the source and destination of a communication, the date, time, and duration of a communication, its type, the communication device, as well as the data necessary to identify the location of mobile communication equipment. These data shall be retained for a minimum of 6 months and for a maximum of 24 months by the providers. Member States should have implemented the directive into national law by the 15th of September 2007. However, the majority of them have failed to timely implement the directive into their national legislation. For data relating to Internet access, Internet telephony and Internet eMail, the directive has foreseen the possibility to postpone its transposition till the 15th of March 2009, an option that 18 Member States have chosen for, including Bulgaria and Romania, who became European Member States after the adoption of the Directive.

3.3.3.2 Implementation Issues

The directive aimed at the harmonisation of the obligations of the providers; nevertheless it is still to be proven whether this goal can be achieved. Various points of the directive are unclear, a fact that makes the implementation procedure of the Member States difficult, while some issues of paramount

[18] European Data Protection Supervisor on the Initiative of the Kingdom of Belgium, the Republic of Bulgaria, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxemburg, the Kingdom of the Netherlands, the Republic of Austria; the Republic of Slovenia, the Slovak Republic, the Italian Republic, the Republic of Finland, the Portuguese Republic, Romania and the Kingdom of Sweden, with a view to adopting a Council Decision on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, Official Journal C 169 , 21/07/2007 P. 0002 - 0014 pt.3,

[19] Press release, The Integration of the "Prüm Treaty" into EU-legislation - Council decision on the stepping up of cross-border co-operation, particularly in combating terrorism and cross-border crime, IP/07/803, 12 June 2007.

[20] Minister Hirsch Ballin (Austria), at the Prüm Seminar, 16.11.2006, available online at http://www.justitie.nl/actueel/toespraken/archief2006/Prum-seminar.aspx

importance for data retention are left unregulated, either intentionally or not. At this point we will only point out a few major implementation issues that trouble the national legislators.

The directive does not include a definition of the term 'serious crime', leaving its definition to the Member State that shall define this term in their national laws. In view of largely variant definitions from the European Member States, given that the definition of the term can be influenced by socio-political situations in each Member State, the Council of the European Union urged the Member States "to have due regard to the crimes listed in article 2(2) of the Framework Decision on the European Arrest Warrant[21] and crime involving telecommunication"[27].

Furthermore, the directive refers to the providers of publicly available communications services or public communication networks. Although the term might seem clear from a first sight a closer examination reveals that many question can arise. What is the role of transit providers or of providers of webmail services? When various providers are involved at different levels of the transmission of a communication, who shall be the one to retain the data? Recital 13 of the directive clearly states that "data should be retained in such a way as to avoid their being retained more than once", but who shall be the responsible of their collection in each specific case?

The directive includes in Article 5 a list with the categories of data that are to be retained, dividing them in three large sub-categories, i.e. fixed telephony, mobile telephony and Internet access, Internet eMail and Internet telephony. However regarding this Article there exist two kinds of dangers: on one hand, the Member States may practically copy the article of the directive keeping its generic wording, which will cause a multitude of interpretation questions, when the directive will be enforced. On the other hand, the Member States may vary significantly with regard to the categories of data to be retained. The aimed harmonisation is also threatened by the fact that the Member States can choose a retention period between 6 months and two years.

At a more technical level the directive does not give answer to important questions regarding the storage and the handover of the data from the providers to the law enforcement authorities. The directive does not ask for the encryption of the data, neither when they are stored nor when they are transmitted to the designated law enforcement authorities. The provider shall decide whether the storage of the data will take place in a centralised or de-centralised way and ensure that the data are kept in a secure environment, which will allow their easy and fast retrieval. ETSI is currently working on the standardisation of the handover interface for the transmission of the retained data from the provider to the law enforcement authority.

3.3.4 Review of the Legal Framework on Electronic Communications – the ePrivacy Directive

On the 13th of November 2007 the European Commission the package of reform proposals to update the regulatory framework on electronic communications. The main documents of the reform are the following[22]:

i. Commission proposal for a Directive of the European Parliament and the Council amending European Parliament and Council Directives 2002/19/EC, 2002/20/EC and 2002/21/EC

ii. Commission proposal for a Directive of the European Parliament and the Council amending European Parliament and Council Directives 2002/22/EC and 2002/58/EC and

iii. Commission proposal for a Regulation of the European Parliament and the Council establishing the European Electronic Communications Markets Authority.

The issues of privacy and information security have been already identified as very important in the Communication on the Review of the EU Regulatory Framework for electronic communications and networks[23] and they cover a part of the Commission proposal amending Directive 2002/22/EC on

[21] Council Framework Decision on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA) (13 June 2002)

[22] The full texts of the proposals are available online at:
http://ec.europa.eu/information_society/policy/ecomm/library/proposals/index_en.htm

[23] COM(2006) 334, {SEC(2006) 816}, {SEC(2006) 817}

universal service and users' rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on consumer protection cooperation (hereinafter 'proposal'). One of the major changes introduced in the Commission proposal relates to security breaches leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed in connection with the provision of publicly available electronic communications services. In such cases the provider of these services shall without undue delay notify the subscriber concerned, as well as the national regulatory authority of the breach. The details regarding the information and notification requirements can be decided upon by the European Commission following consultation with the European Electronic Market Authority and the European Data Protection Supervisor (Article 2(3) of the proposal).

The proposal also foresees detailed provisions on the combating of spam. Service providers would be given the right to start legal action against spammers to defend their own interests or the ones of their customers. In addition, the procedure set up by Regulation 2004/2006 can be used by the national authorities that are responsible for the enforcement of consumer protection laws in order to "reinforce the cross-border cooperation and enforcement in line with an existing Community mechanism laid down by the regulation"[109] and to finally combat the spread of unsolicited communications more efficiently.

Furthermore the proposal recognises the need for adjustments of the definitions in order to conform to the principle of technology neutrality and to keep pace with technological developments (Recital 5of the proposal). Article 3 of the ePrivacy directive is modified in order to include "public communications networks supporting data collection". RFID applications are intended to fall under this provision, as it will be further elaborated in 3.3.5.3.

3.3.5 RFID

3.3.5.1 Introduction to RFID Technology

RFID technology has been known since the beginning of the previous century and was extensively used during the Second World War for the identification of airplanes as "friend or foe". Nevertheless it is considered as an emerging technology due to the fact that it enables a huge amount of innovative applications. RFID tags are not only used in manufacturing, logistics and the retail goods sector, but also in library cards, automotive sector, electronic passports, prisoner or patient armbands, to name just a few. RFID tags used as the medium for collecting and transmitting personal data, as well as tracing devices for the location of natural persons raise questions regarding the privacy rights of the individuals. Notwithstanding the positive impact of RFID technology in innovation, its deployment in several fields of everyday life poses severe threats to the privacy sphere of the individuals that do not know when, how and what kind of information about them is being transmitted at all times. Privacy issues arise when the RFID tag either contains information that can be directly linked to a natural person - thus rendering the information personal data - or the RFID tagged object can be linked to a natural person revealing information about them, such as their location and ultimately allowing identification.

The European Commission has already identified the specific needs regarding the regulation of RFID technology in a Communication on RFID [24] and is working on a Recommendation on RFID that is planned to be adopted in the beginning of 2008.

Moreover the European Data Protection Supervisor published on 20 December 2007 an Opinion on the Commission's Communication on RFID[24]. The EDPS, as the Commission, is in favour of self regulation in the field of RFID technology and sees legislative measures (such as the planned Recommendation) as complementary means to regulate RFID technology and its privacy and security implications. Some of the main points of the opinion of the EDPS is that she is in favour of the opt-in option at the point of sale for commercial products that allow the users to have more control about their data, the "privacy by design" principle and the identification of "best available techniques". Finally the

[24] European Data Protection Supervisor, Opinion on the communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Radio Frequency Identification (RFID) in Europe: steps towards a policy framework COM(2007) 96, 20 December 2007.

EDPS recommends "considering the adoption of (a proposal for) Community legislation regulating the main issues of RFID-usage in relevant sectors, in case the proper implementation of the existing legal framework would fail. After it enters into force, such a legislative measure must be considered as a 'lex specialis' vis-a-vis the general data protection framework. This legislative measure should also address the privacy and data protection concerns that arise in certain RFID applications, such as item level tagging before the point of sale, which may not necessarily involve the processing of personal data"[25].

3.3.5.2 B2B and B2C Applications[26]

In order to examine the privacy risks that relate to RFID technology it is essential to differentiate between its use for Business to Business and Business to Consumer applications.

Business to Business (B2B)

As a rule of thumb it can be said that RFID technology and its respective applications do not raise privacy concerns, when used in Business to Business environments, such as logistics, recycling, industrial processes, etc. However, when an RFID tagged object can be linked to a natural person involved in the business process and is used to monitor her behaviour, things might be different. For instance if an RFID tagged shipment inside a vehicle is linked to the identity of the driver and the RFID movement information is also used to monitor the employee's behaviour, checking for instance the speed with which she is driving, then data protection law comes into consideration as the privacy rights of the driver are involved (see under 1.3 for more detail).

Business to Consumer (B2C)

More "privacy sensitive" are the Business to Consumer applications that entail the use of RFID technology. RFID tags can contain personal data, as in the case of identification documents (e.g. the European Passport), or can be linked to an identified nature person (credit card information about the buyer being stored together with the RFID number of the object just purchased), or can be linked to a natural person in such a way that this person maybe ultimately identified. In both of the aforementioned cases (e.g. RFID tagged shoe that reveals the location or movement patterns of the natural person wearing them) RFID technology raises privacy concerns. Besides the data protection implications that are going to be further elaborated, there are general civil law issues that shall be clarified as a first step. Upon the transfer of the ownership of an object, the full rights about the object must be transferred to the new owner, unless otherwise agreed between the relevant parties. Among such rights vested with ownership is the right to freely determine (i.e. also restrict) the object's ability to pass information to a third person in an controlled or uncontrolled manner, as would be the case, if a newly obtained RFID tagged object would further respond to radio queries about its identification. Exercise of this – basic – right would imply that a kill-function or at least a deactivation option shall be given to the consumer, when obtaining an RFID enabled object, and obviously also requires that the customer is fully informed a) about the presence of RFID tags on the goods and b) about the RFID characteristics such as range, information contained, encryption of such information, etc. Keeping the RFID tag activated shall be only allowed after the informed consent of the new owner. Consumer protection organisations come to similar conclusions and ask for the automatic deactivation (killing) of the tag, unless the consumer explicitly wishes otherwise. In this latter case, the consumer shall be fully informed of the functionalities of the RFID tag and her rights regarding its future deletion or deactivation.

Obviously it might be desirable to maintain some RFID functionality even after the object has changed ownership. The recycling industry, for instance, has a valid argument towards use of RFID to identify "recyclable" objects or components among junk items, so as to take proper disposal measures (e.g. of electrical appliances or refrigeration equipment). In such cases – where public interest may be invoked – mandatory full killing of the tag would not apply. The basic data protection principle of "data economy" would however apply nevertheless and it would call for partial deactivation of the tag so as to keep only the information (and the reading range) absolutely necessary for the recycling purposes.

[25] Idem, par. 92

[26] This part was initially prepared for the needs of the Cluster CERP of European RFID Projects (http://www.rfid-in-action.eu/cerp) by Eleni Kosta and Jean-Marie Willigens (as representatives of the PRIME Project for the activities of the Cluster) and has been modified to fit the form of the Framework V3 document.

As already mentioned above, RFID tags can contain personal data, as in the case of identification documents, or can be linked to a natural person. In both cases the European data protection legislation applies and the collection and processing of the data must comply with the privacy principles and ensure the protection or the rights of the data subject. For instance the processing must be necessary for well defined purposes, the consumer must be informed both about the collection of the data and the presence of RFID readers and the consumer shall have the right to ask the rectification or the deletion of the data, when they are not necessary.

3.3.5.3 Applicability of the ePrivacy Directive

The European legislation for the protection of personal data consists not only of the data protection directive, but also of the ePrivacy directive [36], which regulates specific issues regarding the processing of personal data in the electronic communications sector. The directive aims at protecting the personal data and the privacy of the users of publicly available electronic communications services that are offered via public communications networks. Therefore, in order to decide upon the applicability of the ePrivacy directive, three main issues shall be examined:

- whether there is an electronic communications service,
- whether this service is offered in a communications network and
- whether the aforementioned service and network are public.

As RFID applications do not intrinsically need to be provided over a public network and do not necessarily qualify as publicly available electronic communications services, a lot of confusion exists with regard to the applicability of the ePrivacy directive to such applications. The Commission proposal for the reform of the ePrivacy directive attempts to clarify the issues by complementing Article 3 of the ePrivacy directive as follows: "This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community**, including public communications networks supporting data collection and identification devices.**". This statement is further elaborated in Recital 28 of the proposal, which specifically refers to RFID technology. According to the aforementioned Recital "when such devices are connected to publicly available electronic communications networks or make use of electronic communications services as a basic infrastructure, the relevant provisions of Directive 2002/58/EC, including those on security, traffic and location data and on confidentiality, should apply"[27]. Although the Impact Assessment[28] prepared by the Commission states that "an explicit reference to RFID in the ePrivacy Directive allows for appropriate measures with respect to applications of this communications technology"[29], the confusion regarding the applicability of the ePrivacy directive to RFID applications is still not resolved. The questions what is public or not and when an RFID device is considered as *connected* to publicly available electronic communications networks or makes use of electronic communications services *as a basic infrastructure* will still be in the centre of discussions and will influence the applicability of the ePrivacy directive to RFID and other emerging technologies.

3.3.6 Conclusions from the Legal Perspective

The legal developments in the field of protection of personal data in the European Union are so many and ongoing that a much more pages could be written. In this chapter we presented the major developments regarding the processing of personal data that falls outside the scope of application of the data protection directive. The reform of the regulatory framework on electronic communications, in the frame of which belongs also the ePrivacy directive, is one of the most important issues that will be in the centre of discussions in the following months. The issue of RFID is high in the EU agenda and a Recommendation on RFID is expected to be presented by the European Commission in the beginning of 2008.

[27] Recital 28 of the proposal for the reform of the ePrivacy directive
[28] Commission Staff Working Document, Impact assessment, Accompanying document to the Commission proposals, SEC(2007) 1472, {COM(2007)697, COM(2007)698, COM(2007)699, SEC(2007)1473}
[29] Idem, p.105

The current legal developments illustrate a tendency to regulate areas that were traditionally left untouched. The European legislator deliberately left the processing of personal data under the second and third pillar unregulated, while the current tension shows an attempt for a more uniform handling of such processing. However the collection and processing of large amounts of data by police and judicial authorities and their cross-border exchange present threats that shall be taken into account from the drafting phase of the relevant legislation. PRIME technology and the development of identity management systems can be used to serve the needs of data protection in this field as well. More research, based on the work done, is needed for the development of specific applications that will cover the special needs of law enforcement.

3.4 Privacy and PET Economics

From our research based on case studies and a focus group of privacy experts[30], we find that adoption of PET is usually driven by negative, not positive, concerns. The general attitude is that compliance is not a good motivator for adoption of any form of technology, as can be evidenced by the adoption of regulation-enforcing technologies in other domains, e.g. know your customer rules for banking, technologies for adherence to environmental regulations, etc. We discuss if a business case for PET in a positive light can be made, and what might be the positive drivers for adoption of privacy tools.

We also examine privacy in line with organizational processes and procedures, with the assumption that an organisation cannot maintain a user's privacy preference unless they themselves can assure privacy within their own business processes.

3.4.1 Privacy Adoption Drivers in Organisations

While conducting interviews with privacy experts, when we ask the question whether organisations have some inherent interest in privacy, a list of drivers emerges. These drivers include: compliance with legal obligation, fear of reputational damage from privacy failure, the need to generate trust with clientele, and the promotion of a good corporate practice. Yet if this was truly the case then privacy enhancing technologies would be already implemented everywhere across both industry and government organizations. Reality appears more complex.

There is much doubt amongst experts[31] that there is in fact a well-structured business case for privacy. The traditional drivers are insufficient, in particular:

- Compliance is not taken particularly seriously, since there are so few investigations and even fewer penalties. Recent penalties, however, such as the ruling against Nationwide Bank in the United Kingdom who were fined nearly £1 million by the financial regulator for inadequate response to a data breach, are considered an opportunity for revisiting this concern.
- Reputational and Brand Damage is not an assured result of public disclosures of privacy failures. That is, research and experience show conflicting results on whether organizations actually experience damages to their reputations from data breaches. Amongst experts there is a high level of skepticism that data breach reporting actually hurts companies through a loss of customers, though there has been some research indicating that stock market fluctuations do take place after the announcement of a breach.
- The notion of 'generating and maintaining consumer trust' is a large and perhaps unwieldy goal that is never quite verifiable. While this terminology permeated much of the discussion around eCommerce in the 1990s increasingly there is less being said today about trust. Privacy has not yet emerged as a differentiator in the marketplace — if trust was so important then certainly some organizations would be advertising their privacy-friendly practices quite vigorously.

[30] Privacy workshop in London for experts was hosted by PRIME economic research in May 2007.
[31] Ibid

- There is much faith in the idea that protecting privacy is merely another way of showing good corporate practice, but it is only recently that discussions have emerged about including privacy within corporate social responsibility regimes.
- Participants in the experts workshop mentioned organizations do not currently understand the nature of the risks posed by the processing of personal information. Just as it took organizations quite some time to learn about information security, some believe that this is how we can account for the lack of understanding about privacy. But as storage costs spiral downwards organizations are collecting and retaining as much information as possible — though it is possible that data breaches and other security concerns are finally causing some re-consideration of this trend.
- Another analogy that emerged from discussions and case research is that privacy may follow the same course as 'Total Quality Management' in that privacy can be seen as a means of 'tightening up the ship', in that it will help in better information management. This approach highlights that privacy may not be the 'good' that is being delivered (or sold) but instead the rise in consumer and organizational confidence is the ultimate goal.
  Privacy also falls into that odd area between 'social responsibility' and 'compliance'. While oil companies gain credit for giving money for research into alternative fuels, this is not perceived as a regulatory-burden (at least not yet). Privacy suffers because it is seen as a compliance issue and insufficiently as a good social practice. But in discussions with experts on this matter, they felt that there was much room for growth in this domain, particularly if privacy management is eventual seen as part of an organization's general attitude. That is, if a firm is seen as negligent in the processing of personal information, consumers and other firms should begin questioning whether this negligence spreads to other business domains within that firm such as staffing policies, or even the honoring of warranties.

Therefore the best way to summarize the PET adoption problem space is that:

- There may be a business case for privacy and this could be shown particularly after a privacy failure where a positive demand for privacy emerges and this leads to privacy becoming a differentiator in the marketplace.
- There may not be a business case for privacy per se but there is a business case for better management of information resources within organizations in order to create confidence within the organization, across the supply chain, and with consumers. This better information management is perhaps best done through privacy management.

3.4.2 Business Rationale for Data Collection

People and organisations often adopt identification and authentication in their business activities, even though, as pointed out in Smith and Clarke [124], this is usually not a result of a legal obligation, but often has a purely functional motivation or is even the result of not considering necessity and alternatives. In many situations it is simply convenient for (commercial) organisations to know a person's identity and personal details. Often, personal data are collected that are not directly required for the primary business purpose, but can be used for another so-called secondary purpose, possibly at a later point of time. Frequently, more personal data than actually necessary are requested from customers.

Companies identify their customers and collect personal data for various purposes and reasons [124]. A list of such data collection purposes, provided by a telecommunications provider, is below[32].

Reasons for collecting personal data by businesses

- To better serve their customers. The more a business knows about their customers, their backgrounds, preferences, interests and needs, the better they can match their service offering to these needs and interests, including offering personalised and tailored services.

[32] The list was provided by PRIME partner Swisscom.

- To develop better services and products. Knowledge about customers' needs, interests and behaviours enables businesses to develop new services and products that match these needs better. The more detailed the knowledge about customers is, the better businesses can segment customers with respect to their different needs and develop product portfolios or product suites in which each individual product addresses the needs of the customers in each segment.
- To be able to conduct targeted or personalised marketing. Knowledge about individual customers' or a group of customers' preferences, behaviour and interests allows businesses to send targeted marketing material to these customers or customer segments, (e.g., behavioural targeting) and allows them to make targeted service offers.
- To locate and handle defaulting customers. In case a customer doesn't pay or in case the payment process fails for whatever reason, businesses want to be able to locate non performing customers in order to have them fulfil their contractual obligations, or to seek damages or other remedies. Data necessary for such tracking of non-paying users typically contains the name and address of the customer.
- To recognise returning good and bad customers. Businesses want to recognise returning good customers in order to make them special offers, with special discounts not given to anyone but the best customers, for instance. This promotes customer loyalty and strengthens the relation between business and customer.
- Likewise, businesses may want to recognise returning bad customers in order to limit the service or product offerings or even refuse them entirely (e.g. blacklisting). Businesses also want to recognise returning non-paying customers, customers with bad payment histories, and customers that caused any other problem in order to minimise the risk of losing money over such customers.
- To exclude users who are not in the target groups. Sometimes, businesses only want to sell their products or services to a restricted target group or a limited number of customers. The motivation for such selective customer filtering can be various; the number of items to sell may be limited, the company wants to maintain an exclusive brand image or customer base, or the company knows that a certain type of customer causes the company to lose money instead of make profits.
- To comply with legal or regulatory obligations. Some industries or types of businesses are subject to special legal or regulatory requirements to gather user data. Examples are banks which have to collect their customers' identities and the source of monetary deposits in order to prevent money laundering, or telecommunication companies who have to gather communication data for law enforcement purposes. Also tax regulations might require that data about certain business transactions are collected and maintained for a certain period.
- To mitigate financial risk. Businesses want to limit their financial losses due to unwanted incidents or accidents. For example, companies want to make sure they only enter into business with users that are mature enough to conduct binding contracts. Companies may therefore, gather the age of their customers in order to only serve adults.

All of these interests and activities of businesses increase the earnings and financial benefits through higher service usage, higher market share (having more customers than the competitors) and higher market penetration (leaving aside the least profitable customers who have needs but who don't buy services or products fulfilling these needs).

To address this problem space:

- We discuss how many of these purposes may be achieved if the customer data are pseudonymised or anonymised, for instance with the help of PRIME technology, as will be discussed further in this document.
- We discuss the advantages for companies to use privacy-enhancing Identity Management technologies for minimising or protecting personally identifiable information, as will be discussed further on in this document.

3.4.3 Privacy by Design: Technical and Organisational Assurance Measures

Privacy management in organisations requires procedures to protect data against unauthorized access and usage, which are to some extent analogous to regular internal control measures that safeguard the reliability of data.

In line with this, a distinction can be made between ex ante and ex post measures.

- Ex ante measures create an environment in which data are protected, and so to speak prevent that data are being used in an unauthorised way;
- ex post measures are controls put in place to check whether or not data are being effectively protected.

Privacy (like reliability) cannot be safeguarded by one single measure alone; it will necessitate a collection of measures that collectively provide privacy protection. In other words: a privacy sensitive organisation has to be designed. The collection of measures can include both organisational and technical measures that work in conjunction with each other.

Without proper data management procedures, there are no guarantees that all such personal data will be handled with the same duty of care. Privacy management seeks to maximize the economic benefits of processing personal data by limiting the negative effects illegal or unethical practices. Since the damage from the mishandling or inadvent disclosure of personal data varies across different sectors, applications, and types of personal data it is not appropriate to subject all personal data to the same degree of control. It all depends on the risks incurred, the costs involved and the legal requirements to be applied.

To address this problem space:

- We first address what type of organizations should be most concerned with privacy management, based on both risk assessment and their firm's own ability to enhance privacy in the organization.
- We then examine what overall corporate policies, organisation measures and technical measures companies can take to assure privacy in their business processes. In this assessment, we also examine what role PRIME plays in these assurance measures and where PRIME bridges gaps in existing policies.

3.4.4 The Need for a Business Case Analysis.

For executive decision makers in order to know how much to spend on privacy protection, they should know:

- How much lack of privacy is costing the business?
  - What impact do privacy breaches have;
  - What would the impact be of a catastrophic privacy breach?
- How much do privacy protective measures cost?
- What are cost-effective solutions?

The decision to spend money on privacy has to be financially justified. To comply with legal requirements there is no point in implementing an expensive solution if a less expensive solution would offer the same protection. Beyond the legal compliance, it makes no sense to invest in a solution if it true costs are greater than the value it offers

The investment analysis or the (positive) business case serves as the commercial justification for applying PET. The term 'business case' also refers to its elaboration in a policy document, which

serves as the primary justification and reason for including PET activities in the overall Information Systems project. An investment analysis of PETs requires an answer to three key questions:

- Do PETs make an essential contribution to the policy targets and objectives of the organization?
- What benefits can PETs achieve in the organization?
- What are required investments and structural costs for PETs?

The most important consideration is the extent to which a contribution will be made to the organization's policy objectives. If no contribution or no sufficient contribution is made, the preparation of the business case can be stopped. As the basic driver for investment in PETs is their potential to avoid privacy incidents, an upfront privacy risk analysis is needed.

The application of PETs may result in different type of benefits. If it leads to a reduction in costs, then the benefits can be measured and, therefore, are quantitative. For example the application of PETs may lead to a so-called migration of controls, where procedural and organizational measures are replaced by technical measures for data protection. Qualitative benefits are hard to express in monetary terms and tricky to measure, e.g. the positive image generated by the application of PET.

As for the third question, the costs of PETs vary because of the range of possible PET controls that can be implemented. The emphasis in data anonymisation lies on the one-off investments and less on the structural costs. However, when data are separated, different domains have to be created, the data model usually has to be modified, and there is more often a need for customization to implement the PET option. Furthermore costs are to an important extent determined by the question whether the implementation of PETs is an integral part of design and development of a new information systems, or whether PETs have to applied to legacy applications. The latter is of course is much more expensive and may even sometimes be hardly possible.

A thorough business case will assure that all these considerations are taken into account and serve as basis for decision making.

3.5 Social Developments

3.5.1 Privacy is a Balancing Act

Privacy is a fluid, continually changing thing [70] . It is influenced by developments in society, which makes privacy a 'balancing act'. The socio-cultural developments that effect the value of privacy can be divided in three levels: developments on the level of society 'as a whole' (macro-level), developments on the level of interactions between individuals and businesses or institutions (meso-level), and developments on the level of interactions between individuals (micro-level).

Macro level developments provide us with a frame in which the meso-level developments and the micro-level developments take place. A first interesting development on the macro level is the increasing emphasis on risk and safety. Whereas societies have made a shift from safeguarding their member's security in the late 1800s, towards the ensurance of values like welfare, progress or freedom in the early 1900s, the pendulum now appears to swing back to security and risk. A renewed interest in safety and risk can be observed [111]. A consequence of this shift seems to be that (Western) states increasingly feel a need to gather information to reduce risks (we have entered what has been coined the 'risk society'). Information and communication technologies (ICTs) obviously play an important role here, because collection of (personal) data can be an instrument to gain insight in risks on the one hand, and a means to reduce risks and to ensure safety on the other ([96], [80]).

A second macro level development is that all actors in society increasingly make use of ICTs. Life, and its environment, increasingly becomes digitised and connected [110]. Indicators of this are, for instance, the enormous increase in broadband internet access in recent years and the growth of online services (both private, like eCommerce, and public, like eGovernment), although not all European countries have an equal share in these developments ([23], [34]). For example, 37.1% of the Dutch respondents of the PRIME survey use the Internet more than 20 hours per week against 34.5% of the

Belgian and 33.4% of the British respondents.[33] With an expanding use of ICTs, the use and dependency on information, including personal data, increases and more people and institutions are confronted with the collection and application of information. Also, the amount of information to be distributed and processed will increase further.

As a matter of fact, the increasing adoption of ICTs in Europe can partly be attributed to the emphasis on the 'knowledge society', a third macro-level development. According to the 'Lisbon agenda', the development of this knowledge society is necessary to create growth and employment in Europe and requires, amongst other things, the spread of ICTs and the promotion of new technologies [60]. The emphasis on knowledge, research, and development can contribute to a convergence of technologies, which can make it increasingly difficult to control data in the future [29]. It can also lead to a changing application of technologies and an increasing use of and reliance on information. Additionally, it can privilege the value of knowledge and innovation (free flow of information) in its relation with other values, like privacy.

The fourth relevant macro-level development is that the use of ICTs by actors in society means that the need for a presence of the physical body is decreasing, when relations are originated and maintained. This 'disembodiment' requires new approaches to identification: classic trust tokens cannot be used in the virtual context and 'time-space' is coordinated in different ways [81]. The use of eMail, for instance, does not require a co-presence of the body and whilst communicating by eMail, classic attributes that facilitate identification like voice, body language or clothing cannot be used. Disembodiment can lead to an increasing collection of data, as societal actors assume having more (personal) data will help to establish trust [76]. Furthermore, disembodiment can facilitate the use of pseudonyms and false identities, which influences aspects of honesty and deception [39].

As a fifth macro-development, new technologies are effecting the role of the individual in society. On the one hand, community ties can not only become more geographically dispersed, weak, and fluent, but also only specialized in content and withdrawn from the public space [143]. On the other hand, new technologies make it easier to connect with large numbers of people, can foster meetings with people that otherwise would have been forgotten, can effectuate contact with more diverse others, and can increase the control and self determination of individuals in social interactions [143]. Therefore, the online world is different from the offline world. The shift towards networked societies and networked individualism [144], requires information sharing and retention of information between multiple actors in different locations and in several roles. Also, societies and communities that are more fluent and difficult to comprehend can result in an increasing collection of data, when actors and institutions assume this decreases risks and increases accountability.

The last macro-level development, mentioned here, is the increasing cross-border dimension of social interaction, economic relations and institutional collaboration. As a result, surveillance becomes 'globalised' ([82], [81]). Infrastructures and organisations are transnationally organised, which results in the move of data across several countries [48]. A globalised economy also leads to the situation wherein companies share data between globally dispersed business units. Moreover, the outsourcing and integration of business units requires the share of (personal) data between these transnational organisations. Another effect of the global economy is that if companies need to comply with national legislation (e.g. corporate governance codes), this can encourage the retention of (personal) data from business units in other countries as well. Additionally, citizens and consumers are increasingly facilitated to commence relations that exceed borders: both online (e.g. transactions on the internet) and offline (e.g. traveling abroad). This can increase the use and storage of personal data in multiple countries. Another cross-border aspect is the level of collaboration between governments concerning the retention, use and sharing of data. Examples here are agreements on the processing and transfer of passenger name records [28] and the request for globalisation of legislation relating to privacy [48].

More concrete, trends can be pointed out on the level of interactions between the individual and businesses and the individual and the government. A first meso-level development is the increased use

[33] The PRIME survey is a large scale online survey conducted in the Netherlands, Belgium, and the United Kingdom in 2006 and 2007. Due to time and budget constraints, samples of students at universities and colleges of further education were chosen. A total of 7635 students participated in the survey. For more information, see the PRIME Survey Report which is forthcoming (by: Oomen, I.C. & Leenes, R.E. (2008)).

and collection of customer information by businesses. On an expanding scale, customers are being 'activated' by commercial organisations to influence the product or service that is being offered. Furthermore, online services are becoming user-centered and user-generated, so, by their participation, users create the added value of a service ([97], [147]). An increased interaction with users, however, requires the collection of information about them and their preferences, more than the 'classic' collection of customer data. And with disembodiment in commercial relations, it seems that market parties are inclined to collect data in the assumption that this strengthens trust and security (see also section 3.4.2). On top of this, the identity and reputation of market parties is more difficult to determine by the consumer as dubious vendors can more easily enter the market with the use of ICTs [90].

All in all, customer information is increasingly becoming a determining factor and strategic asset for companies. This appears, amongst other things, in the fact that almost every online company collects personal information from individuals [132], for instance by asking them to register. But also IP addresses and cookies (less traditional personal data) are used for constructing customer records. Moreover, new technologies make data collection and data sharing more easy through web forms, cookies, and ubiquitous technologies for example. This creates the possibility to achieve more intimate customer relationships [44]. However, data collection and data sharing can lead to the practices of profiling, behavioural targeting, social sorting, dynamic pricing, and target advertisements ([76], [132], [40]). Customer information is also used for customer tracking, data mining, and imposed personalised services. In addition, the existence of an active market for customer information increases the possibility that detrimental behaviour is not limited to the company that has initially gathered the information ([132], [76]). This makes it difficult to determine the accountability of market actors in the case personal information has been passed on to other parties.

Other meso-level trends are visible in the relationship between citizens and the government. A first development is the rise of standardised and centralised electronic public records, wherein data from citizens is collected and stored. Large databases are under development, like biometric databases, electronic children's files, ID databases, and healthcare records. Although these records can provide the citizen with effective services, reduce risks, and increase safety and efficiency, public records also present difficult privacy challenges [40]. For instance, the records can be difficult to maintain, manage, and protect and can eventually lead to "function creep", if the information is used for unintended purposes in the future ([70], [121], [148]).

Another meso-level development of the last years is the increase in surveillance measures to ensure the safety of citizens and to prevent crime. Some of these measures are the use of video cameras and smart ID cards, the screening of communications, and the examination of the location of an individual (see: [129], [78]). These measures can, next to their benefits, negatively effect the position of citizens in the sense that people can, for instance, be excluded from services and can be discriminated by the unequal use of surveillance techniques.

Other government measures can also impact the privacy of citizens. Democratic instruments, like voting machines and web-based voting-advisers, can have an impact on the security and confidentiality of citizens' democratic opinion. The recent abolishment of voting machines in the Netherlands due to privacy and security concerns – after having been in operation for well over twenty years – is an interesting case in point (see: [43]). Also, the use of personal data is essential to support the increasing use of electronic public services (e.g. ePortals), but can provide different levels of government with sensitive data. This use and collection of data by the government can cause a tension in the trust between citizen and government [80], especially when public services are joined.

Finally, some short remarks concerning the privacy of employees. In the relation between employee and employer, the collection of personal data is increasing as well, even though in many European countries there are strict workplace privacy regulations. For instance, employees are being tracked and located by instruments like RFID and GPS, and, in other occasions, employees are surveyed by the means of keystrokes, telephone calls or video camera's. In many occasions, workplace surveillance contributes to a safe and efficient organisation and can decrease health risks and fraud for example. But it needs to be stressed that workplace surveillance can also influence the public-private sphere, can invade the privacy of the employee, and can decrease creativity and productivity inside an organisation ([86], [40]).

For many people, the internet is a place where they can engage in social interactions [88]. On the individual to individual level (micro-level), online interactions between individuals are facilitated through chat, virtual communities, personal pages, web logs, profile sites, MUDs (Multi User Domains), MOOs (MUD Object Oriented), and MMORPGs (Massive Multiplayer Online Role-Playing Games). Many of the online interactions between individuals can be performed anonymously, for the internet was built 'without a way to know who and what you are connected to' [13]. No less than 46.6% of the PRIME survey respondents have one or more anonymous email addresses. In these anonymous interactions, people don't have an idea who they are dealing with. However, many actors do attach their real identity to their online identities and thus personal information is shared (33.3% of the PRIME survey respondents don't use pseudonyms). For instance, nicknames are rarely changed, because reputation is associated with it (the majority of PRIME survey respondents use their nicknames or pseudonyms for years and many respondents reported to have never changed their nickname or pseudonym), and users' accounts can reveal personal information through personalised email addresses and digital signatures that contain details. Furthermore, personal pages and web logs are most of the time related to particular persons and often reveal pictures, personal interests, hobbies, or relations. Personal information can also be uploaded and shared through videos and photos, and, in addition, online characters in games and virtual environments can resemble the real world identity of a person ([83], [84], [31]). In online social interactions, personal information is shared, because social capital, reputation, and display of connections are important for the individual (see: [38]). However, there is a friction between these aspects and the privacy-related issues that can occur in online interactions. Specific characteristics of technologies make it more likely that certain privacy risks will occur. For instance, people leave (everlasting) digital prints or digital traces on the internet, which can be altered in some significant and potentially damaging way and can be distributed to many and many thousands of others in a matter of minutes. The information can thus be decontextualized and recontextualized without a trace and the individual no longer has control over the information once available on the internet. Even if personal information is deleted at its source, it can already have been replicated elsewhere beyond control of the individual. Moreover, time is irrelevant. An individual can engage in a social exchange without the other person being online at the same time. Also, the physical distance, determining social relations in the real world, becomes irrelevant and makes interaction with people from all over the world possible. The final, and already mentioned, characteristic of anonymous interactions is that that a name can be fake and other characteristics, that normally give information (e.g. physical appearance, body language, facial expressions, and gestures), are absent [88]. Due to these specific online aspects, privacy related issues like 'identity theft', 'identity deception', 'flaming', and 'trolling' can easily occur. In identity theft, personal information is obtained and used in a variety of fraudulent ways to impersonate the victim ([127], see: [71] and [72]). Identity deception is taking another identity, which can vary from gender swapping (i.e. pretending your are a male instead of female or vice versa) to changing all personal attributes (e.g. gender, name, age, occupation, and place of residence). Gender swapping can be relative harmless, but it can have serious forms as well if persons use an other gender for a long time in an intimate environment. Flaming mostly occurs in chat or in virtual communities and is characterized as the gratuitous and uninhibited expression of remarks containing swearing, insults, name calling, and hostile comments [84]. Flame responses are typically generated as a response to other posts or to users posting on a site and the flame responses are often an attack on the person self. Trolling is a more serious form of flaming because a person infiltrates a certain group and pretends to be one of the members. After a while, when the trust of other members is gained, this person starts to 'act out' by disrupting discussions, giving bad advice, and damaging the feeling of trust in the group [39]. Identity theft, identity deception, flaming, and trolling can have far reaching consequences for people and their online social interactions with others. It is seen as dishonest behaviour [87] and as an infringement on people's privacy, for people feel betrayed because their most intimate lives are intruded [84]. So, in the online interpersonal relations, several aspects of privacy can be affected. First, the control over limited access to intimate relationships can be invaded. Second, the protection of one's personality and dignity can be threatened, especially because of identity theft. And third, managing personal information is more difficult with online social interactions [126].

The several societal developments on a micro, meso, and macro level that are mentioned in this paragraph, lead to a shift in balances in (informational) privacy. On different levels and in several interactions in society it is visible that personal information is increasingly being collected, processed,

retained, and possibly used in a harmful way. It becomes more difficult to control the reliability and dissemination of personal information and, in addition, people are often not in the position to detect and terminate infringing actions. Identity theft and identity deception are possible and personal information can be retained, decontextualised, and recontextualised. Hence, privacy is eroding slowly. Although a certain level of transparency in society can be beneficial, the lack of privacy can have a severe negative impact on the individual and on society as a whole. For privacy creates the context for many social relationships, and is necessary to ensure a number of societal and individual values.

3.5.2 The Need for Privacy

There always has been an innate need for privacy, which can be observed by the fact that even the animal world and primitive societies seem to contain aspects of seclusion and 'social distance' [146]. Developments in society may force us to reconsider the notion of privacy and the instruments necessary to achieve privacy, but it is clear that privacy contributes to many values, like pluralism, creativity, democracy, mental health, and the capacity to have meaningful relations [55]. Knowing that we cannot provide a complete and exhaustive list of arguments for privacy here, the need for privacy can however be displayed by stipulating how privacy contributes to some individual and societal values.

Firstly, privacy creates the conditions to develop and maintain intimate and various relations. It makes it possible to adjust the information that is given to specific relatives ([112], [65]), which enables life and its relations to be multidimensional and controllable. People furthermore sometimes just need to escape from daily life [85], as relationships without privacy can lead to hostility and irritation. In other words; even life with 'sporadically' unbearable persons becomes impossible without withdrawal into privacy [130].

Additionally, a certain level of privacy is a prerequisite for the values of autonomy, accountability, and trust, because having autonomy over the way people portray themselves to others makes it possible to act in a moral way and to adjust their appearance to social norms. Autonomy implicates accountability of the individual for his or her actions, e.g. considering the information they choose to disseminate to others ([65]). If there were no privacy, people could make no autonomous choices regarding their identity, could not be held accountable for the information they disperse, and do not need to be trusted, for all information about them can already be acquired.

Another value that is served by privacy is the value of having a 'second chance'. Privacy makes it possible for people to rely on a certain level of 'forgetfulness', which means that they will not always be confronted with their former actions and/or mistakes. The ability to have privacy and a 'fresh start' makes it possible to alter one's identity throughout life, to develop and evaluate the 'self', to avoid (future) stigmatisation, and to have an identity which is aligned to the current behavior and perceptions of the individual [6].

Moreover, an important aspect of privacy is that it contributes to equality and homogeneity in society. Sharing information can lead to a power imbalance between the data subject and a data controller, for personal information can be used as a basis for current and future (unknown) actions of the data controller. These actions may also include discrimination, blackmailing, revenge, and stigmatization. Privacy can serve as a countervailing power against collectors of personal data (viz. the State, press, relatives, and data processing companies), and their potential unwanted use of personal data.

What is considered private is culturally and socially defined and varies from context to context. It is quite possible that no single example can be found of something which is considered to be private in every culture. Every individual 'establishes a unique balance between privacy and social participation' ([116], p.216). The only common feature of all private things is that they are aspects of a person's life which are culturally recognied as being immune from the judgment of others [65]. This difficulty to define common aspects of privacy does not mean, however, that privacy needs to be regarded solely as being a concern for the individual. Privacy is also a common, public, and collective value - more than just an individual right - and does not necessarily conflict with society. The commonality of privacy can be found in the observation that every individual values privacy to some extend. Privacy is furthermore a public value in the sense that it has value to the democratic political system. Finally, privacy is a collective value in the sense that every individual can experience privacy-infringement [116].

3.6 Conclusions

The previous sections have focused on developments that, taken as a whole, facilitate a gradual erosion of privacy. This seems by and large a natural process of technological advancement (e.g., [70]). Information sharing and monitoring are promoted stronger by technology than information shielding. As technology evolves, we gradually adapt ourselves to its possibilities and we also slowly downgrade the reasonable expectation of privacy [70].

To correct the imbalances described above and give the individual more control over her personal data, while at the same time promoting other interests, requires a reassessment of the way personal data is handled. A balance has to be found between the various relevant interests in a flexible and transparent way. These interests themselves fall into four categories: (1) perceived individual tangible interests; (2) perceived intangible interests; (3) economic or business tangible interests; (4) policy interests (freedom, public interest, etc.).

Given the complexity of the issues and interests involved, single technical solutions will be insufficient, as will be a strong reliance on only non-technical measures, such as legislation. Privacy protection requires different modalities of regulation (see also [77]). This corresponds with the outcomes of the PRIME Survey, as respondents perceive that privacy protection is mainly their own responsibility, but they also think it can be increased by more legislation and enforcement by the government, more computer software (i.e. PETs), and by organisations who should be clearer about what happens with their personal data. Privacy protection requires technical components as well as more soft aspects, such as trust establishing mechanisms, changing attitudes by organisations, and correcting people's perceptions. With respect to the technical components, there is a strong tradition on fundamental research on privacy-enhancing technologies for minimising or avoiding personal data since the early eighties (e.g., [18], [19]). The research and development of PETs has grown and gotten more attention over the last years. There are several privacy-enhancing technologies available and in use today, including anonymising tools (e.g., Anonymizer, JAP, TOR, Mixmaster), privacy policy languages to express a companies privacy policies and the user's privacy preferences (P3P), anti-spyware, spam filters, software for detecting and deleting cookies, personal firewalls and encryption tools. However, these techniques and tools provide solutions limited to certain aspects of the problem, i.e. they are rather isolated technical solutions, addressing, for instance anonymity, but neglecting accountability in case of misuse. They also tend to focus on one side of the equation, the user or the service provider. Although there are industry and standardisation initiatives for developing identity management solutions enforcing some fundamental privacy principles (including Microsoft's InfoCard, IBM's Higgins as well as the ISO/IEC JTC 1/SC 27 initiative - see also section 1.2), there are currently no practical solutions based on a comprehensive approach that integrates user side and services side tools for strong privacy protection. Furthermore, existent PETs have a low adoption rate, as they usually lack ease of use and as there are not enough perceived benefits for end-users and organizations for deploying them.

For effectively addressing privacy and reestablishing user control, a holistic approach has to be taken to develop comprehensive solutions that technically enforce strong privacy, are based on the European regulatory and legal framework, and are socially acceptable and desirable, economically exploitable, intuitive and user-friendly, deployable by applications.

The PRIME project aims to deliver these comprehensive solutions. The next chapter will describe the vision the project has for such solutions.

4 Vision of PRIME

Compared to the offline world, individuals in today's information society increasingly lose transparency, sovereignty and effective control over their personal spheres; their right to privacy is at stake as illustrated in the previous chapter. Privacy is a basic human right as well as a pillar of democracy, which requires that citizens can freely articulate their opinions and participate in democratic processes without the threat of being monitored and sanctioned.[34] This requires the careful handling of personal data. Personal data is an essential asset because it represents power. It is therefore essential to protect this asset to preserve the individual's autonomy.

PRIME envisions that individuals in the information society can communicate and use services in a secure and reliable way while keeping sovereignty over their personal spheres under the same or better conditions than they had previously. PRIME will develop privacy-enhancing identity management tools that restore the individual's privacy in the online world, while simultaneously combating its misuse and supporting legitimate law enforcement interests.

PRIME takes a holistic approach and investigates, and subsequently integrates functional, legal, social, economic requirements and HCI principles for privacy-enhancing identity management in the PRIME tools that comply with the needs of users and service providers, enforce legal privacy principles, are socially accepted, trustworthy, user-friendly and economically exploitable.

Central to realising this vision are the following technical design principles [105]:

> "**Design must start from maximum privacy**": The base system is designed to maximise the individual's control over personal data. By default, interactions are anonymous: partners know neither the identities, nor the location of each other. Individuals can choose pseudonyms to link different interactions to each other, bind attributes and capabilities to pseudonyms, establish end-to-end secure channels between pseudonyms, and digitally sign messages. Whether or not interactions are linked to each other or to a certain pseudonym is under the individual's control. Privacy and anonymity is also ensured with respect to system operators. Users can have a multitude of (temporary) pseudonyms thereby safeguarding their personal sphere and being able to operate in different social spheres. Anonymity revocation is available under strict conditions for resolving disputes and supporting law enforcement.
>
> "**Explicit privacy rules govern system usage**": On top of the anonymous or pseudonymous base system, technical policies determine how to use the system, including policies for trust establishment and reputation establishment, as well as privacy preferences and privacy authorisation policies.
>
> "**Privacy rules must be enforced, not just stated**": Privacy policies are enforced at the receiving end by technical means. The use of personal data and the enforcement of the policies produces enough evidence so that users can actually trust the enforcement and proper use of their personal data.
>
> "**Privacy enforcement must be trustworthy**": Trust is motivated by building on a trustworthy computing platform and by using assurance methods. Furthermore, external trust mechanisms are implemented that audit data controllers' systems with respect to compliance to legislation and agreed privacy policies.
>
> "**Users need easy and intuitive abstractions of privacy**": To be useable by non-expert users, intelligible and intuitive user interfaces are needed that are based on metaphors and mental models that hide technicalities like pseudonyms, linkability and privacy policies.

[34] Remember that the basis for the American Constitution, the Federalist papers where written anonymously, and more recently, the informer known under the pseudonym 'Deep Throat' played an important role in unravelling the Watergate scandal.

"**Privacy needs an integrated approach**": All technical components are integrated into user-side and services-side tools for privacy-enhancing IDM.

"**Privacy must be integrated with applications**": PRIME is integrating the results of its research into legacy and new applications.

Besides, PRIME tools also provide functions for helping users to track their data releases as well as online functions allowing and helping users to exercise their basic rights to object to data processing, and to access, rectify, block or delete data under certain circumstances.

In order to achieve this vision, not only technological development is required to create the tools and techniques outlined, but also an extensive deployment strategy has to be elaborated. This involves studying and developing non-technical measures supporting the wide use of PRIME technology, such as end-user tutorials for raising awareness, standardisation initiatives, and explicating economic and social drivers, as well as legal support measures.

Historically, privacy has always been a particularly important right for European citizens. In recent years, this right is being undermined by technical advancements, combined with economically and politically motivated driving forces. The advanced technology developed by PRIME can help revive privacy. Not only for the sake of furthering privacy and the goals it promotes, but also to enable trust and confidence in the Information Society.

Privacy enhancing technologies represent a potential enabler for business, as they provide competitive opportunities, especially for privacy-sensitive applications, as they manage the risk of regulatory non-compliance, reduce the scope and costs of audits, and as they allow to meet the customer's privacy preferences and to achieve optimal relationships with them.

The implementation of privacy enhancing technologies, such as PRIME, will convince more citizens, consumers, businesses and governments to adopt ICTs in their daily operation and bring the promises of the Information Society, including economic productivity and combativeness, new businesses and employment, increased democratic participation, to full fruition. It will also increase European leadership in the area of privacy and privacy enhancing technologies [46].

PRIME will accommodate a migration path from existing products, so that PRIME solutions will fit into the reality of the market's development.

5 Towards the PRIME Solution

5.1 Introduction

This chapter provides a holistic view on PRIME's solution for meeting the PRIME vision and its legal, social, economic and technical ingredients and prerequisites. For this, section 5.2 first presents an integrated view on the legal, social and economic requirements for a PRIME solution. In section 5.3 we also briefly describe an Identity and Access Management Maturity Model with PET extensions, which allows evaluating an organisation's ability to adopt PRIME. After having discussed these prerequisites for a PRIME solution, the PRIME solution as such is finally described in section 5.4 in form of a holistic privacy management framework.

5.2 Requirements for the PRIME Solution

This section encompasses a description of key requirements for privacy-enhancing identity management systems, which the PRIME solution that is described in the subsequent sections of this chapter aims to address. A complete elaboration of the legal, social, and economic requirements is drawn up in the PRIME Deliverable 'Requirements V3' [10]. This section summarises the key legal, social and economic requirements from that Deliverable and puts them into relation to each other where possible. In particular section 5.2.2 provides and integrated perspective on requirements that commonly arise from the law and social sciences. Also the table in Appendix A puts the economic requirements discussed in section 5.2.4 into relation with legal and social requirements.

This section starts with a summary of basic legal data protection principles, and then continues with the common legal and social requirements, a social 'user adoption' requirement, and economic requirements, which all facilitate a successful implementation of privacy-enhancing technologies.

5.2.1 Basic Data Protection Principles

As mentioned above, the legal requirements are thoroughly analysed in the Requirements V3 document. In this subsection, we will make a summary of the basic data protection principles in order to provide the reader with an overview of the legal framework that applies to privacy enhancing identity management. The legal requirements that have a strong social motivation will be discussed in the next subsection.

- **Principle of fair and lawful processing (Art. 6(1)(a) Data Protection Directive):** According to the principle of legitimate purposes personal data must be processed fairly and lawfully. The collection of the data shall be based on a legal ground and the right to data protection shall be balanced against other interests involved in the processing of the data [75].
- **Principle of finality / purpose limitation (Art. 6(1)(b) Data Protection Directive):** The finality or purpose limitation principle provides that data controllers must collect data only as far as it is necessary in order to achieve the specified and legitimate purpose they pursue, and cannot carry out any further processing which is incompatible with those purposes.
- **Principle of data minimisation (Art. 6(1) Data Protection Directive):** Another basic data protection principle is the principle of data minimisation, according to which the processing of personal data should be limited to data that are adequate, relevant and not excessive. Consequently, data controllers are obliged to store only a minimum of data sufficient to run their services.
- **Principle of data quality (Art. 6(1)(d) Data Protection Directive):** The data quality principle provides that all personal data "shall be accurate and, where necessary, kept up to date". The data controllers are imposed with an obligation to take every reasonable step to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected are either erased or rectified.

- **Principle of conservation (Art. 6(1)(e) Data Protection Directive):** The data conservation principle states that personal data shall not be kept for longer than is necessary for the purposes for which this data was collected. According to this principle after achieving the purpose for which the data was gathered, it should be rendered anonymous or destroyed.
- **Principle of notification to the Supervisory Authority (Art. 18 Data Protection Directive):** The data controller must notify the respective national data protection authority before any data processing operation is carried out. The Directive leaves to the Member States the possibility to simplify the notification procedure or to waive it altogether in certain situations.
- **Principle of Restricted Data Transfer to Third countries (Art. 25 Data Protection Directive):**The transfer of personal data to countries outside the European Union is only permitted if the third country in question ensures an adequate level of protection. Exceptions to this rule are possible according to Art. 26.

5.2.2 Common Legal and Social Requirements

The PRIME social and legal requirements present similarities, as they can be linked to collective values and principles, like autonomy and user control. Therefore in this section we have made a description of the most important common legal and social requirements that shall be respected in the design phase of a privacy-enhancing identity management system. These combined requirements are: 'information to the user', 'consent'; 'users' right to access the data', 'right to rectify, block, and erase the data', and 'data security', which are analysed in the following subparagraphs.

5.2.2.1 Information to the User

The first requirement, 'information to the user', is an important prerequisite for fair and lawful collection and processing of personal data. Providing information to the user (the data subject) ensures compliance with the existing data protection legislation, and has many other positive aspects and benefits both for the data subject and the data controller. Moreover, disclosure of information is one of the key prerequisites for *user control* through self determination, which successively is a core principle for privacy-enhancing identity management systems and both national and European data protection regulation [94]. Establishing user control creates satisfactory interactions, human well being, and diverse relations, to name just a few positive consequences (see [62], [65], [131], [112]). Information to the user is also of importance because only when a user is informed ex-ante a service can be considered fair, which raises the willingness of people to continue in a relationship [30]. In addition, ex ante information is a precondition for users to enforce their personal rights assigned by data protection regulation.

The data protection directive 95/46/EC foresees that the data controller shall give some information to the data subject, according to Article 10. This minimum information that has to be provided to the data subject is the following:

a. the identity of the controller or his representative,

b. the purposes of the processing for which the data are intended,

c. any further information if this is necessary to guarantee fair processing in respect of the data subject, such as the recipients or categories of recipients of the data, whether replies to the questions are obligatory or voluntary, as well as the possible consequences of the failure to reply and the existence of the right of access to and the right to rectify the data concerning her.

This information has to be provided to the data subject at the time -or before- the data is collected. If disclosure to a third party is envisaged, Article 11 provides that the information must be provided at the latest when the personal data will be disclosed. The directive excludes the right of information in cases where the disclosure to a third party is made for statistical purposes or for the purposes of historical or scientific research, and when "the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by [national] law" (Article 11(2) data protection directive).

The information that is given to the user is seen both as a right of the data subject in order to ensure that she is always informed about the processing of her personal data, as well as an obligation of the data controller to inform the data subject respectively. In practice the obligation to inform the data subject, is seen as a major duty of the data controller, as the data subject very often is ignorant of the fact that processing of some of her data is taking place, let alone the details regarding the processing.

The fact that disclosure of information is both a right of the user as an obligation of the data controller, indicates that knowing when personal data is being processed is an important issue. *Consciousness* of a data subject is a prerequisite for a solid 'social contract' between a data subject and a data controller. It is also a key condition for human autonomy and human dignity, and it contributes to transparency in the unequal power relation between data controller and data subject. Mostly, the party that shares personal information is the weak party in this relation. Individuals should be taken seriously and thus need to be informed about what is being done to them. In this respect, consciousness deserves special attention when computing becomes ubiquitous, boundaries between organisations are blurring, and technologies are converging (cf. [25], [81].) By creating consciousness the rise of a panoptic-, or surveillance society, in which human behaviour is normalised due to the possibility of continuous surveillance, can be averted [52].

Next to consciousness, *comprehension* is another important aspect in the process of informing the user about data collection. Users need to understand what is actually happening when data is being collected. This comprehensibility is a difficult task because of the varying need for information between persons and social groups, and because there is always a risk of information overload [59]. Comprehension of the information that is shared with the user, however, is important to facilitate a true choice and to give truly informed consent to data collection. It avoids mistaken disclosure of information, false information sharing, and users regret, for instance. In this respect, it should also be noted that a privacy-enhancing identity management system and its shared information needs to be *consistent*. Many actions regarding the collection of data lie in the future and thus, there is always a risk of future misrepresentation of a digital identity. People, preferences, and situations change. Users need to be able to anticipate to these changes. This creates trust in the application through 'situational normality'. Or, in other words, when things go 'weird', people lose their trust in a system [89]. In many occasions, the personal data that has been collected can be used to create a profile of the user, which is highly determinative for her current and *future* identity. To make sure that users can predict and reckon their future representation, Identity Management Systems need to provide a 'glimpse' into the future, e.g. by showing the normal line of operation and by informing the user about the consequences of her actions.

Summarising; next to the legal requirements, users should be able to:

a. understand the application;

b. have access to (concise) user documentation and

c. understand the consequences of their actions and the normal line of operation.

As a final remark it also needs to be noted that complementary information to the user (in the form of markers, warranties, and seals about the organisation) can contribute to the *trust* of a data subject in the data transaction parties (further elaborated in 5.2.2.5).

5.2.2.2 Consent of the User

One of the grounds for legitimate data processing is the 'unambiguous consent' of the data subject. Consent, which can be defined in different ways, is of major importance because it can change an unlawful act into a lawful one [145]. It thus makes the difference between an infringement and an allowed use of personal data. Consent and the related right to oppose to processing of personal data, strongly relates to fundamental human values such as individuality, dignity, civility, and autonomy. Consent should be voluntary and in most of the cases shall be revocable (see also 5.2.2.4). Moreover, influences of force, fraud, incompetence, and paternalism need to be rejected. In this respect, hierarchical relations deserve special attention.

According to the data protection directive, the data subject's consent shall mean any "freely given specific and informed indication of her wishes by which the data subject signifies her agreement to personal data relating to her being processed" (Article 2(h) data protection directive).

It is very important for the data controllers to interpret correctly the aforementioned legal provision in order to avoid violations of the data protection legislation and mainly to examine what *freely given, specific* and *informed* means. A *freely given* consent shouldn't be counterpart of an advantage or subject of negotiations on behalf of the data controller. The consent needs to be *specific*, meaning that it should be given for a specific and identified scope. Finally, it needs to be *informed*; the user shall get the appropriate and sufficient information before the collection of the data and such information shall be in clear language and of course in a language that the data subject understands. A highly debated issue is whether consent can be expressed in an opt-in or in an opt-out way. It is necessary that "there must be some form of communication whereby the individual knowingly indicates consent" [136]. This can be expressed by ticking a box[35], or sending an eMail or subscribing to a service [136]. For the processing of sensitive data, i.e. data that reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership or data concerning health or sex life, the data subject shall give her *explicit* consent, although Member States may prohibit the processing of sensitive data, even with the consent of the data subject.

It shall be noted that the definition of consent explicitly rules out consent being given as part of accepting the general terms and conditions for an offered electronic communications service.[36] However in current practice consent is usually exactly given in the general terms and conditions of an offered service, which presupposes the processing of personal data. The picture gets even blurrier when the consent of the user is given in an environment that allows no or minimal user interface, such as in the case of most emerging technologies, like RFID, Bluetooth, etc.. Ambient Intelligent environments are based on the processing of personal data and obtaining the consent of the data subject is not always taken into account in the designing phase of these systems.

Following from the requirement of consent, *choice* is an important social condition for true privacy-enhanced identity management, because consent implies a possibility for the user to choose whether or not to engage in a service and subsequently to choose how her privacy is addressed in different services. An online identity is composed of different kinds of information, and when service providers use a 'take-it-or-leave-it' approach (viz. without different privacy options), it is not possible for users to withdraw specific information from the focused attention of others. This results in the ineffectiveness of PETs because users can then still be exposed to forced disclosure of information and to unwanted profiling and stigmatisation. Individuals need to be enabled to choose *by themselves* the way they are portrayed to others [93], instead of being bound to predetermined identities and predetermined judgments. However, for the sake of motivation and feasibility, choice should not be exaggerated, but moderated and limited [67].

Finally, next to choosing the information shared and consenting to data collection, individuals also need to be able to set the boundaries in which their data is being used. This *confinement* can be divided into the aspects of purpose of use and security measures. There is a possibility that data controllers define the purpose of use and access to data too broadly or incomprehensively for the user. Therefore, the user should be enabled to define purpose and access, especially because of the already mentioned possibilities of blurring boundaries between organisations[37] and the convergence of technologies which can result in data leakage to others and/or use of data for purposes it was not collected for ('function creep', see: [148], [81], [29]).

[35] Recital 17 ePrivacy Directive

[36] Article 29 – Data Protection Working Party, Opinion on the use of location data with a view to providing value-added services, adopted on 25 November 2005, 2130/05/EN (WP 115), p. 5. More analysis on this specific issue and specifically on unsolicited communications see Article 29 Working Party in its Opinion No 5/2004 on unsolicited communications for direct marketing purposes under Article 13 of Directive 2002/58/EC, adopted on 27 February 2004 (WP 90)

[37] Both private and public.

Thus, consent must be freely given, specific, and informed, and users need to be able to clearly determine and choose the kind of information shared, the purpose of use, and the access of others to data.

5.2.2.3 The Users' Right to Access the Data

A central notion of user control on her personal data (see 5.2.2.1) would be useless if the data subjects would not be able to *inspect* whether their actions with regard to data collection have the desired effects. Even though ex-ante requirements of consent and information to the user result in the fact that users are able to assess the processing of data in the future, they do not fulfil entirely because it is difficult to predict the future use of data. Data can be interpreted or presented wrongfully, and users can make mistakes or regret their earlier decisions. Access to data is therefore necessary to inform users about the compliance of the data controller to agreements and law, to inform about the correctness of data, and to inform about the possible mistakes or harmful behaviour of the data controller. Just like 'information to the user' contributes to *ex-ante* transparency, the right to access data contributes to *ex-post* transparency and strengthens and levels the relation between data subject and data controller.

The data protection directive grants various rights to the data subject with regard to the processing of her personal data. The right of access to her collected personal data reads that every individual whose *personal data* are been collected and processed has the right to obtain from the data controller:

a. confirmation as to whether or not her personal data are being processed and information at least as to the purposes of the processing, the categories of the data concerned, and the recipients or categories of recipients to whom the data are disclosed,

b. communication to her in an intelligent form of the data undergoing processing and of any available information to the resources and of any available information as to their source.

Where any automated decisions (as defined in Article 15 data protection directive) are involved, the data subject has the additional right to be informed about the logic involved in any automatic processing of data concerning her.

All the aforementioned information must be available to the data subject 'without constraint at reasonable intervals and without excessive delay or expense' (Article 12 (a) data protection directive). In addition and as regards how the right of access is exercised, an ideal situation would include both online and physical access -the latter realised at the physical address of the data controller. However, in cases where physical access would entail disproportionate efforts and costs on behalf of the data controller (or if the data collected is disproportionately little), it is arguably accepted that the right of access can be exercised only through online means. In such a case however, the controller shall ensure via strong authentication mechanisms that the person requesting some information about the processing of personal data is the one entitled to do so, in order to avoid cases of identity fraud, identity theft etc.

Access and inspection contribute to the fairness of processing of data and decreases the power imbalance between the strong party (data controller) and the weak party (data sharer) in a data collection process. It is thus a countervailing power. It needs to be noted that the user should also be able to inspect and control data collection throughout the *chain* in which a service is being delivered. The user should thus not only be able to inspect the actions of the collector of data, but also the actions of the other actors in a service chain with regard to her personal data. Often, services are provided by combining the efforts of several organisations. The telecommunications sector for instance, has multiple parties engaged in the provision of one single service [152]. Furthermore, business processes and the data processing involved can be outsourced to other (specialized) parties. Users should therefore not only have insight in the phase of initial data collection, but also for instance in the phases of subscription, payment, and integration of a service.

5.2.2.4 Rectification, Erasure, and Blocking of Data and the Right to Object

People can make mistakes or regret their decision to disseminate personal information. Initially, one can be tempted to disseminate personal information, as the benefits of information sharing are much clearer than their disadvantages [128]. Negative effects of data disclosure may, however, occur later in time, when people encounter unwanted use or abuse of personal information. Also, people need to have the ability to decide to continue or modify one's behaviour, especially if situations change, or if used

personal information is wrong or interpreted wrongfully and does not comply with purpose of use of expected representation.

A right of access in the broad sense includes a right to rectify, erase, or block the data that relate to her, in cases where the processing does not comply with the requirements of the data protection directive (for example, the data controller's collection of personal data is disproportionate to the purposes), and in particular when the data at issue are incomplete or inaccurate (Article 12 (b) data protection directive). A common instance where the data subject exercises her right to rectify the data is when her name is misspelled and she asks for the rectification. Furthermore, in the course of *ex-post* control over her personal data, the data subject has also the right to object (Article 14 and recital 45 of the data protection directive) to the collection and processing of her personal data.

However, it shall be pointed out that the aforementioned rights can be imposed upon the data controller, only when the data subject has a legitimate right to do so, and at the same time the data controller does not have an overriding right to process the data. It shall be borne in mind that the consent of the data subject is only one of various reasons, according to which the processing of personal data can take place, so the right to object can not for instance be exercised in front of a data controller, who deems that the processing is necessary for the performance of a contract to which the data subject is party.

Nevertheless, Article 14 of the data protection directive stipulates the cases where the right to object can be exerted. Firstly, when the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller or in a third party to whom the data are disclosed and when the processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights for fundamental rights and freedoms of the data subject, Member States are obliged to grant the data subject a right to object at any time on compelling legitimate grounds relating to her particular situation to the processing of data relating to her, save where otherwise provided by national legislation. When there is a justified objection, then the processing instigated by the controller may no longer involve those data.

Secondly, the data subject can object, on request and free of charge, to the processing of personal data relating to her which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses.

The ePrivacy directive perceives in various situations the right to object as withdrawal of consent. Therefore, the specific right is implicitly mentioned as a right to object to the installation of cookies, to the processing of traffic data processed for the purpose of marketing electronic communications services or for the provision of value added services, the processing of location data other than traffic data, to have her data available in directories of subscribers and to the processing of her personal contact information in order to receive unsolicited communications. In all the aforementioned cases, the data subject is given the right to refuse the provision of services or in cases where she has already accepted them, to withdraw her consent.

All in all, the requirement of access to information would lose its value if subsequent actions cannot follow from the inspection of information. Thus, *ex post* user control by erasing, blocking, and correcting information is closely related to access and inspection. This requirement can serve a societal need for forgetfulness; sometimes, people will feel the need to get a 'fresh start' or 'second chance' [6]. Moreover, a world in which people cannot make mistakes and nothing is forgotten is not a world conducive to the development of democratic and autonomous individuals [69], even though there sometimes is a need to hold users accountable for the information they share and even though the responsibility for the quality of data lays at the data controller. *Ex-post* user control by blocking, erasing, and rectifying information is therefore a balancing act, between what is (legally) necessary to achieve accountability of the user, correctness of data, and the (legal) possibility to provide the user a control tool which can complement the data controllers' obligation with regard to the quality of data.

5.2.2.5 Data Security

The aforementioned socio-legal requirements noted that the user needs to be enabled to control personal information by being informed, giving consent, and have access and the possibility to block or change information. An important prerequisite however is a secure infrastructure, without which these actions are meaningless. Therefore the data controller needs to take appropriate security measures, as is mentioned in regulation. From a social perspective, this security requirement can furthermore be viewed from the perspective of *trust*: an important aspect of online transactions (see [61] or [49]). Trustworthiness and security are not the same, but many users will not be skilled to asses the security measures taken by a data controller and therefore, markers of security are also of importance.

Data security, is requiring data controllers to take 'appropriate technical and organizational measures' (Article 17 (1) data protection directive) against unauthorised or unlawful processing, and accidental loss, destruction or damage to the data. To the extent that this principle covers the security requirements and robustness of the network itself, this principle overlaps with the security and confidentiality requirements laid down in articles 4 and 5 of the ePrivacy Directive (Directive 2002/58/EC). Taken as a whole, this principle imposes a statutory obligation on data controllers to ensure that personal data are processed in a secure environment. This means that the data controllers must consider the state of technological development and the cost of the implementation of any security measures. Bearing in mind these factors, the security measures that are adopted by the data controllers must ensure a level of security that is appropriate to both the nature of data to be protected and the likely harm that would result from a breach of this principle [15]. It follows that, the more sensitive the data, the more adverse the consequences of a security breach would be for the data subject, and therefore more stringent security requirements should be put in place. This is especially the case as regards the processing of health related data. In any case, the data controllers should implement appropriate security measures to ensure that non-authorised personnel are not able to gain access to personal data. In addition, security precautions would suggest making back-up copies.

Security measures are of importance to ensure the earlier mentioned boundaries of data processing, determined by the user (see 5.2.2.2). Without appropriate security measures, confinement of data processing is not possible. There is also another relevant (social) aspect when discussing security: Infrastructure and transaction partners need to be trustworthy. Security can be an aspect of this trustworthiness. Thus, not only should an organisation handle a secure transaction of data, they should also make these risks and their measures transparent to the user. The user needs to recognize the reliability of a technology and the trustworthiness of an organisation. This is difficult to achieve because many users are no experts in the field of technology and security, and online transactions lack face-to-face interaction.

Trust is commonly conceived of as the assumption that another person, organisation, and its technology cause no harm, and that it is in the interest of the data controller to attend to the interests of the data subject. By its very nature and by the differences in social context, trust is defined different amongst social groups and individuals. However, some generally regarded markers of trust -like the use of security seals- can contribute to the trustworthiness of an application and the organisation that uses the application (see forthcoming Requirement V3 Deliverable). These markers can come from well-reputed organisations, and should not only apply to the specific security measures (which are difficult to comprehend), but also to information about sources, providers, affiliations, and certificates of the data processor. A broad use of markers is necessary, whereas there is a general problem with regard to trust in technology: the information about security and trustworthiness needs to *be tailored to the context of the (non-expert) user*.

Trust in technology will often be combined with the trust in the partners one engages with. This is also important considering the adoption and use of a privacy-enhanced service. For the sake of trust and the adoption of a technology, complementary markers about reputation and brand of a data controller/service provider can therefore also be of importance [90].

5.2.3 User Adoption Requirement

The combined social and legal requirements mostly show similarities in the field of user control and self determination, which is important to ensure privacy on the individual level. However, there is also

another important social aspect to be mentioned with regard to the development and deployment of privacy-enhancing identity management systems. It is the requirement of 'adoption'.

Privacy is a situated, context related and multi-layered concept [151]. This means that amongst others, social and individual factors determine privacy preferences and the use of PETs. It also means that PET-use and PET-preferences are dependent on the situation in which information needs to be shared and depend on what kind of information is being shared. It is a major challenge to develop a system that is flexible enough to comply with all these demands, especially because there can be tension between adoption of a PET, user control, and the social need for flexibility.

The current social reality creates conditions for a privacy enhanced system of identity management.[38] This means that requirements like 'information to the user' and 'access to data' should be aligned with the current *zeitgeist,* to increase adoption. Until now, PETs have not been able to bring about a large adoption. This can be attributed to the user, which could be regarded as unmotivated, not skilled, or otherwise unable to adopt technology. However, it can also be attributed to the privacy-enhanced technologies, which did not take into account the many social conditions, like social differences and people unwilling to pay for PETs.

Social- and context values matter. PETs need not only to be used by the privacy-concerned, technically-skilled individuals, but also by the privacy-naïve, and unskilled individuals. A 'digital divide' (cf. [33], [138]) in the field of privacy needs to be averted by creating a PET that can be used by everyone. Therefore, privacy-enhancing identity management systems should take into account the following aspects, which need to be interpreted contextually: A) social settings, like individual preferences, the kind of data to be shared, the situation in which data is shared and other specific preferences of social groups (e.g. age, gender, nationality); B) skill level of users; C) (legal) accountability of the user in specific instances; D) markers, warranties, reputation, and other information to ensure the users' trust and; E) willingness to pay for a PET.

Without adoption by the users, a PET is useless. So, combined socio-legal requirements need to be complemented with issues of adoption of such technology. Furthermore, organisations and institutions should, next to the user, adopt PETs as well. This is, amongst other things, elaborated in the following section.

5.2.4 Economic Requirements of Privacy Measures into Business Processes

Given this section examines the economic aspects of privacy management, we will focus on the view from the service provider (data controller), rather than the individual (data subject), since the economic impact of privacy is more clearly definable on the service provider side of the equation.

From our research [107], we see a relationship between the need for privacy and the level of information intensity in an organizational process, including organizational maturity to handle privacy along with the associated risk levels of the process. Potentially high information intensity in the value chain can be a large number of suppliers or customers with whom the company deals directly, a product requiring a large quantity of information in selling, a product line with many distinct product varieties, a product composed of many parts, a large number of steps in a company's manufacturing process, a long cycle time from the initial order to the delivered product [103].

If there is information intensity, there is also a higher possibility of risk associated with privacy and information loss or modification. The ability to adequately handle privacy risk is also a maturity function of how the organisation organises both technological and organizational measure to ensure privacy in the process. Organisational measures are the measures for designing the organisation and for the processing of personal data (such as segregation of functions, instructions, training and calamity plans). Technical measures are the logical and physical measures for information systems (such as access control, storing the use of data). Technical measures can also be Privacy Enhancing Technology (PET) measures. This would include an identity protector in the design of systems that would permit individuals to interact anonymously with service providers. There are several specific techniques for introducing an identity protector into an information system. Specifically, encryption techniques

[38] i.e. age, gender, skills with technology, political history, experiences, etc.

involving digital signatures, blind signatures, digital pseudonyms and trusted third parties are used, as well as role-based access and encryption.

The starting point is to develop a corporate privacy policy departing from the organisation's objectives, based on which a policy can be formulated for processing personal data. The formulated policy, such as corporate methods of utilising passwords or other identity mechanisms, must give tangible form to specific measures and procedures for the processing cycle of personal data. Defining tangible measures and procedures occurs after thorough risk analysis, listing the threats to which processing of personal data is exposed. Within this context the strong and the weak points of data processing are laid down. The risks together with the strong and the weak points of the processing organisation and a cost-benefit analysis, based on the defined privacy policy, result in a carefully considered choice for the organisational and technical measures to be taken.

An organisation's management can determine the way in which technical and organisational measures are taken in order to safeguard the protection of personal data. It can adapt this to the existing organisation and further detailing of administrative organisational and technical measures and procedures to safeguard (automated) data processing. Based on the existing set of control instruments, the management can further implement the legal requirements in an effective and efficient way. Unfortunately, the law currently does not impose on organisations any compulsory set up with regard to these technical and organisational measures. However, an organisation can protect themselves and their users from a regulatory perspective via a privacy audit with an established audit firm. In carrying out the Privacy Audit, the auditor firstly investigates whether the organisation has been set up in a way that makes possible to comply sufficiently with the legal conditions (the design). Next, the auditor assesses the existence of measures and procedures taken by the organisation in order to assure the compliance with the legal requirements. Last but not least, the auditor concentrates on testing the operation of the measures concerned over a predetermined period to check compliance. The auditor's assessment criteria, which must be considered when deciding whether the privacy measures are appropriate, include:

- state of the art in technology;
- the costs of implementation;
- the risks, regarding processing, nature and volume of data.

Appendix A shows technical and organizational measures to be taken for adding value in the process design for privacy and shows how they relate to the legal and social requirements for PRIME discussed above. Those requirements were derived in the PRIME internal Deliverable F2, which also discusses PRIME's ability to contribute to those requirements. The conclusions of F2 are based on our case studies, the work of our auditor from KPMG, and the contribution from one of the PRIME developers in response to our work.

5.3 Identity and Access Management (IAM) Maturity Model with PET Extension

To examine under what conditions an organisation would adopt PET into its business processes, we explored how an IAM maturity model can be adapted to examine privacy adoption maturity in organizations.

During the last decade several maturity models have been developed in specific research areas such as business IT alignment, software development and information security. All of these models have one thing in common; they all describe the maturity of one or more processes within an organization. As a basis for this IAM maturity model, a number of existing models were examined. In summary, we examined the maturity models of consultants Nolan Norton, the Capability Maturity Model (CMMi), and INK (Instituut Nederlandse Kwaliteit) maturity models, and all had some influence on this IAM model.

The processes we have defined for IAM are shown in Table 1:

Identity and Access management			
Processes		Technologies	
Authorisation Management	Activity aimed at the coupling of users to the already assigned rights to access information and resources through the possible use of authorisation models.	Field of requirements For **Trust** **Federated Identity Management**	Field of requirements For **Personalisation**
User Management	Activity aimed at management of the complete e-identity lifecycle and assigning and revoking of authorisation		
Authentication Management	Assigning the correct means of authentication to the user and the management of means of authentication and authentication profiles		
Provisioning	Propagation of user accounts by means of an automated process or manual process to IT objects.		
Monitoring and Audit	Providing insights into the user accounts, authorisation and process execution. Achieved by using logging, permanent auditing and reporting.		

Table 1 Identified Identity and access management processes and technologies

In our IAM model, authentication management and provisioning are mapped on access management since access management deals with authenticating credentials and controlling the access to resources. Given the choice of processes, mainly from work from KPMG [137], we then place maturity phases into these processes, and develop an IAM maturity model shown below in **Error! Reference source not found.**.

Based on the phase characteristics depicted above and the description of the phases provided by the different model, the following general phase descriptions are induced:

Phase 1: Only few processes have been defined and processes are conducted on an ad hoc base.

Phase 2: Processes that seem to work and be in order, are repeated.

Phase 3: Processes are standardized and documented to review if they are executed accordingly.

Phase 4: Performance and success are measured and quality measures are done

Phase 5: Processes are systematically improved with the help of quantitative feedback of results, test results and innovative ideas.

Authentication Management	No authentication means	Arbitrarily formulated authentication requirements (authentication means are provided, adjusted and detected on user request)	Authentication requirements based on a one time survey	Authentication requirements based on continuous risk analysis	Authentication requirements based on continuous risk analysis and are continually adjusted
User Management	Double and inconsistent entries because of chaotic and ad hoc processes	Entries can be double but they are consistent	Central registration, limited user group, manual procedure	Central registration, controlled authorisation processes, manual procedures	Central real-time controlled authorization sources, automated procedures
Authentication Management	No authorisation matrixes, authorisation is defined ad hoc	Authorisation matrixes defined but are not updated	Authorisation matrixes are updated periodically	Role based access control used for critical applications	Role based access control for all applications and continuous updated authorisations
Provisioning	Manual processing locally	Limited automated unreliable processes locally	Limited automated but reliable process locally	Limited automated and reliable for multiple sources	Automated and reliable for multiple sources
Monitoring (Audit)	No responsibility delegated into a AO/IC organisation	Sporadically delegated responsibility of AO/IC	Partial delegation of responsibility to AO/IC	Full responsibility to AO/IC	Full responsibility to AO/IC with periodic reporting
	Immature	**Starting up**	**Active**	**Pro-Active**	**Top Class**

Table 2 Conceptual Identity and access management maturity model

The filled out maturity model can in turn be translated into a more general description of maturity phases for IAM in general. This means that the whole IAM situation is described per maturity phase. Describing the situation in general leads to a more practical and understandable image of the Identity and access management processes.

In the Whitebook on Privacy Enhancing Technologies by Kroon et al. [74], all is stated that PET is composed out of several technologies divided in four different PET steps (shown in Figure 1). With the help of IAM, PET tries to minimize the use of and access of sensitive personal data. Secured Access however is only the first step for PET. Privacy Enhancing Technologies also strive to segregate sensitive information in order to secure a person's identity. Not only segregation however is used to achieve this goal. Depending on the organizational information needs, information can also be immediately removed after use or not even registered in the first place.

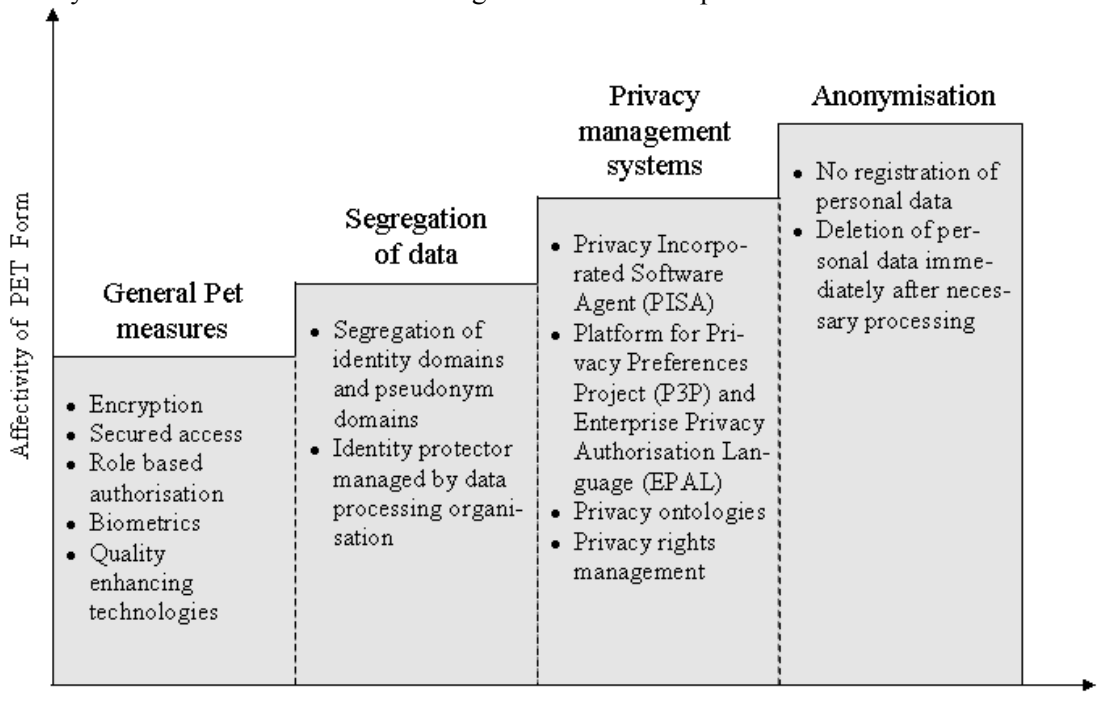

Figure 1 Staged Affectivity of PET including used technologies per stage

For the implementation of PET, certain maturity of the organisation is required. It is highly unlikely that immature organisations will implement PET, let alone that these organizations have any awareness of privacy protection. The level of maturity for IAM is a strong indication for the introduction of PET in an organization.

Next to user management, authentication management and authorisation management, provisioning and monitoring and audit can also play an important part in a PET implementation. For instance when a central database of information is accessed by different organizations provisioning (automated or not) can play an important to keep user accounts for that database up to date at the different locations. Monitoring and Audit plays an important role when reviewing the current status of user accounts and controlling if data is accessed by authorized users only. Thus depending on the requirements of the organisation on its PET implementation a certain level of maturity is needed for the relevant IAM processes. By combining the PET steps and the maturity model the maturity model can predict when PET will be used in which stage of development of the organization.

Based on this model it is predicted that PET will be applied by organizations in the Top Class and Pro-Active maturity level, with the exception for organizations that update authorisation matrixes periodically (organisation at the level: active). There are exemptions for those organisation that belong to the category of (micro/mini) SMEs where trust is a critical success factor, like in the medical profession, barristers, notaries etc. Although the processes mentioned in the maturity model are non-existent, it may be expected that those SMEs will protect personal information of their clients encrypted or will use rudimentary PET tools.

5.4 Towards a Privacy Management Framework

This chapter describes the PRIME solution in more detail by means of a privacy management framework. A privacy management framework presents a solution for data controllers and processors. There are two motivations for introducing such a framework. First, each organisation has its specific reasons and requirements for handling personal data (see section 3.4). While it is difficult to come up with specific procedures for managing information privacy in each organisation, the absence of a generic management framework for information privacy means that many organisations and organisational units are "re-inventing the wheel" for partial solutions and learning individually through trial and error. Second, in order to implement the vision (see chapter 4) and enforce an organisation-wide privacy policy, IT architects need a privacy management framework to assess the changes required in their systems. The implementation of the privacy principles mandates a privacy management solution that manages and coordinates the usage and processing of personal data in multiple IT systems spanning several business functions.

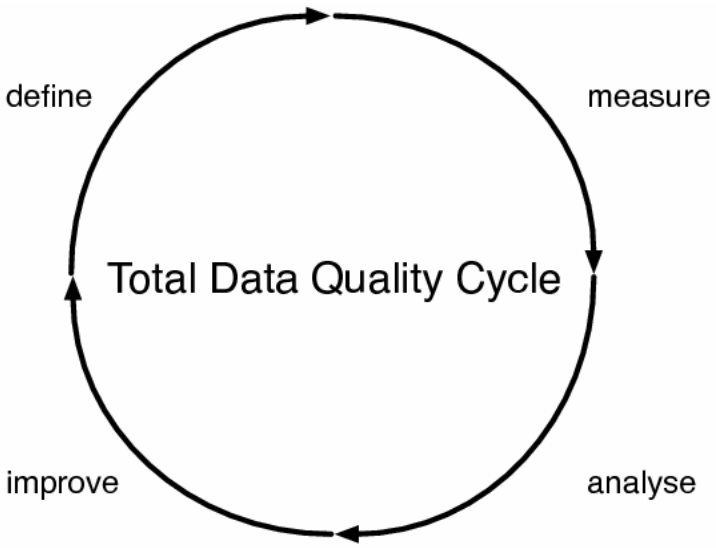

Figure 2 Total Data Quality Management (TQDM) Method

Framework models are often employed in software engineering to illustrate the relationship between components in a system. Many enterprises find it useful to have a framework model, such as the IT Infrastructure Library (ITIL), when managing the IT services within their organisation. Deming's quality improvement cycle: Plan, Do, Check, Act is widely adopted as a basis for such framework models [32]. The Total Data Quality Management (TQDM) Method [140] also uses the Deming quality improvement cycle as the basis for improvements in Information Quality (see Figure 2).

Industry practitioners have developed best practice guidelines for security management, but so far, no guidelines exist for privacy management. Ongoing discussions within CEN/ISSS Data Protection and Privacy Workshops strive to develop a common European set of voluntary Best Practices for data protection management (see Figure 3, [16]).

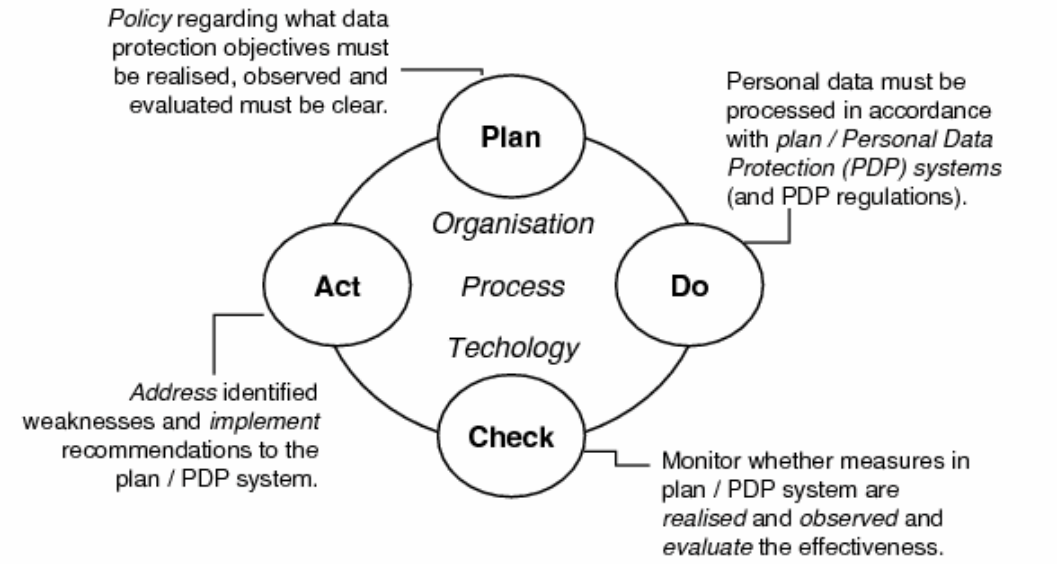

Figure 3 The personal data protection management control cycle (according to CEN/ISSS)

In order to ensure that the corporate-wide policy is followed whenever personal data is processed, architectural innovation is required on a technical level. The privacy management framework complements the architecture by describing the privacy management processes on an organisational level. A privacy management framework addresses specific management processes for information privacy within organisations. It applies the principles of quality management for privacy management within organisations so that compliance can be monitored and improved continually. It provides a basis for organisations to assess their compliance with industry best practice, and to benchmark their level of compliance relative to competitors.

In this chapter, a sketch of a privacy management framework based on the PRIME architecture is presented. It will be embedded in the life cycle of an online service[39] to illustrate the kind of decisions a developer of an online service has to make during development, operational life and termination of the service. After describing the service provider's view on the development cycle, the focus is shifted towards the user side's perspective. Here we will see many similar processes, albeit with a slightly different interpretation. The user-side view focuses on the processes performed by the user and her identity management system (IDM). The chapter will conclude by describing the role of the user interface in realising some of the functions of the IDM.

[39] By online service we mean services that make use of the internet, as well as mobile services, such as GPRS or GSM services.

5.4.1 Service Provider Side

This section starts with outlining the online service life cycle that any new service follows from its inception until its retirement. It describes the privacy management framework, which consists of the processes that primarily play a role in the operational phase have to be performed by the online service. Yet, to prepare for the proper operation of the service, decisions shaping and impacting the processes have to be made in the earlier stages of development. These decisions are influenced by considerations from a Social, Legal, and Economic (SLE) perspective. This section describes the various stages in the life cycle and discusses key issues and decisions to be made from an SLE perspective. The section will then focus on the core processes operated by the service from a privacy point of view, the data and metadata processes. Finally, it will map the functions on PRIME components.

5.4.1.1 Service Life Cycle

An organisation[40] intending to deploy a PRIME system in their environment will be challenged with the questions of what to do when. The life cycle presented in this section (see Figure 4) aims to provide an outline that describes different activities and their inputs/outputs from the environment and indicates when to perform these activities.

Life cycle approaches are not new and in fact the life cycle depicted in Figure 4 builds on existing life cycle models, primarily on the security life cycle proposed in [55], and is expanded with findings from business administration [108] and software engineering [68]. The innovation lies in the attention to SLE impacts and how they are accounted for. It thereby reveals the holistic approach taken in the PRIME project. It facilitates understanding how PRIME specific process and activities can be integrated into new and existing services. Figure 4 shows that we divide the life cycle into five phases, that contain processes that consists of activities. Dependent on the need in each phase, multiple iterations of the processes are executed. The activities and processes adapt and use components, such as the architecture and toolbox, that are developed in PRIME. In addition we acknowledge many environmental interdependencies on all layers, of which the social, legal, and economic effects are the most prominent.

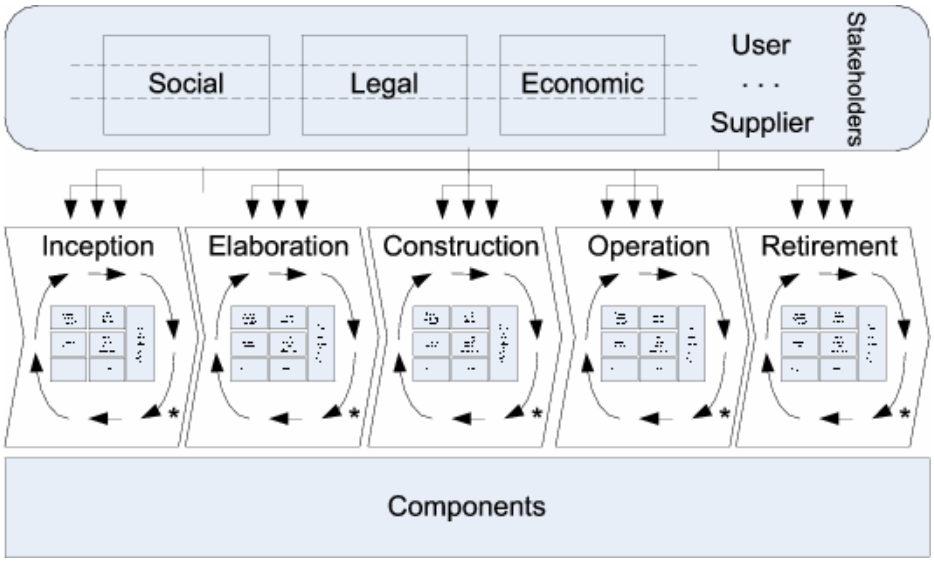

Figure 4 Life cycle of a PRIME enhanced system

Figure 4 shows (at the top) that the various stakeholders in the service, including (intended) users and suppliers of services and data, provide (socio/cultural, legal and economical) input in the form of requirements, constraints, needs, opportunities, etc., in all stages of the service's life cycle. SLE aspects therefore not only play a role in the form of initial design requirements, but have to be taken into account

[40] Within this chapter we will use the general term organisation to denote data controllers, such as businesses, companies, enterprises and governments. User is used to denote the client, customer or user of services provided by these data controllers, although depending on the context also other terms may be used.

throughout the life cycle of a service and also on all levels of development. In the discussion below, we will address some of the relevant SLE issues, without aiming for completeness, which is well beyond the scope of the current framework.

A service provider intending to deploy a privacy solution such as PRIME in their environment will be challenged with implementation questions. If the service provider is designing a new system or a new business process, then logically, already at the inception and elaboration phases (see below), privacy measures should be part of the system design. If a service provider is adding privacy measures to an established business process (e.g. during the operation phase), then it is a bit more complicated as to where privacy measures should be implemented within the process, as discussed below. For both scenarios of new or established processes, when a system is ultimately retired, how the data is handled in terms of privacy policy measures also needs to be addressed taking legal, social and economic requirements into account.

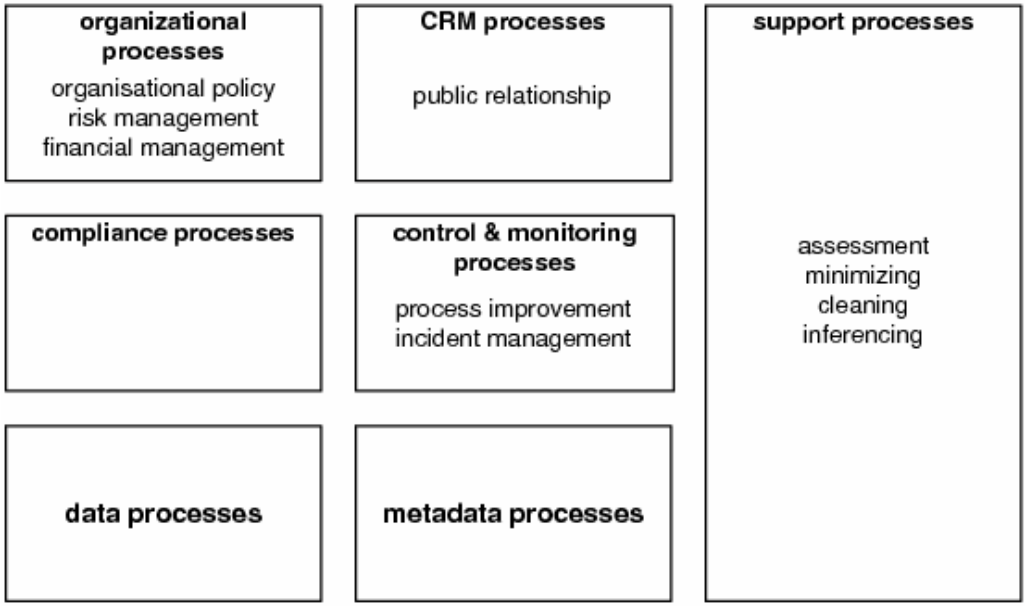

Figure 5 Top level processes in the PRIME life cycle

5.4.1.2 Phases

From a privacy point of view, the service under development has to iteratively perform a number of processes in its operational phase. These processes are depicted in Figure 5. They are described in detail in section 5.4.1.4. Although the processes are primarily performed by the online service when in operation, their configuration and implementation takes place throughout the service's life cycle. This means that the developers have to consider them also in the early stages of development, as well as after retirement of the service. The focus and depth of the attention will differ from phase to phase as we will show below.

> **Inception.** In the inception phase, the prospective service provider develops the first plans for the new service. The focus is to tentatively determine the scope of the service, the intended users, the benefits to both the users and the service provider and to look for obvious barriers. Typically, in this phase only a quick scan with respect to these issues will be performed with limited resources.
>
> Even in this early stage, all processes in the process model need to be considered as they may hint at potential problems later on. For instance, if one considers developing a completely anonymous service, compliance with new and pending data retention regulation[41] may require special attention later on. Realising this early on will help shape the service and may prevent unpleasant surprises. The principal processes to consider in this phase are the Organisation and

[41] As discussed in section 3.3.3.

CRM processes because they provide insight into the risks, benefits, costs, and the way users of the service are managed.

On the basis of the assessment of the intended users, the kind of service, etc., and a comparison with successful and failed similar services, the SLE factors can be investigated. This can be done in a rough SWOT-analysis[42] where a number of SLE factors can be probed. Potential showstopper (preventive problems) have to be identified and potential remedies have to be listed. From a business (economic) viewpoint, a cost-benefit analysis (as discussed in section 5.2.4) has to be performed, as well as an initial strategic planning: what kind of resources would be required, when, and how to get them. From a socio-cultural perspective, characteristics of the intended audience are listed and associated with the requirements of the service. Among the questions to address are: What is the intended audience and what are their expected or desired demographic characteristics? What kind of (personal) data do I need to run the service successfully? Would the target audience be willing to provide these? Would the users see the data as sensitive, would collection, profiling, sharing, etc., be problematic for the users? Would it be necessary to distinguish different kinds of users, for instance because a significant difference in (privacy) attitudes is to be expected? Do I require active (chat, action, transaction) or passive (browsing service) users? What would this mean for the level of control they require in the service? From a legal perspective, one has to get an understanding of the legal context in which the service will run. Questions to address here are, for instance: Does the service require individual contracts with users? Are there special liabilities imposed on the service provider? Are cross/multi-jurisdictional issues to be expected, for instance because of differences in areas such as contract law or intellectual property law in the various countries where the service will be offered? Which kinds of regulation are relevant for the intended service?

Also the use of PETs and specific PET features in relation to the questions raised above need to be explored. From a technological point the viability of the PRIME solution has to be confirmed. Under the assumption that a PRIME-based solution is an appropriate choice, one needs to investigate how user acceptance changes with a PRIME-based solution for the overall service and how PRIME technologies and its PET features will be accepted. Finally, the effectiveness (for example, cost effectiveness, business enabler ...) of the PRIME technology in the specific application has to be investigated.

The result of the inception phase is a first business case that allows to determine whether the project should terminate, or be elaborated in more detail.

Elaboration. If green light is obtained to pursue the service, details of the service have to be further developed in the elaboration phase. In this phase a detailed planning of activities in the project has to be generated and requirements, especially with respect to personal data processing, including abstract data handling policies in natural language, have to be defined. All of this is still at a fairly high level of abstraction; elaboration can still end in a no go decision. All process areas have to be elaborated to a some extent, identifying what is necessary for successful operation.

With respect to PRIME, in the elaboration phase the relevant PRIME components are selected. Subsequently these selected components are integrated into the design and architecture of the overall service. This also requires that the generic workflows described in section 5.4.1.4:‘Data Management Process’ and 5.4.1.4:‘Metadata Management Process’ are instantiated for the specific application. In other words, the specific personal data workflows through the organisation are designed. During elaboration it might also be necessary to develop a prototype which shows how the PRIME technology works in the intended environment.

The SLE impacts for the requirements will come to equal share from all three domains. The business planning initiated in the inception phase will refocus on tactical and operational issues. For the planning, many project management activities, such as team development and resource management, have to be considered. The costs and relative benefits of using various privacy options have to be considered. This analysis interlocks with the social analysis, and to a lesser extent with the legal

[42] Strengths, Weaknesses, Opportunities, and Threats

analysis. For instance, can CRM as envisioned be properly done without collecting personal data? Would running a privacy-friendly and secure service attract different numbers of users than a less privacy-friendly service? Will this affect the capability to attract advertisers, if required? The social aspects to address include considering how users will perceive themselves and their identities in relation to the service. Would they consider it to be natural to operate under pseudonyms (as in chatrooms), or would they feel more at home interacting under their civil identities, as may be the case in a government run policy forum. In more abstract terms, social ontologies and semantics have to be constructed: which kinds of identities, concepts, roles, trust tokens, reputation identifiers, etc., are required to model the user experience? What are the risks of people appropriating other people's identities? Is it possible to prevent this kind of ID theft? Can third party credentials be used in this respect?

The legal questions to address mainly follow from the answers to the kind of questions addressed in the socio-economic analysis. If personal data needs to be collected and processed, the relevant legal provisions have to be studied in detail considering general national data protection legislation as well as possible domain specific regulation (e.g., health services have to comply with many domain specific rules). Also European regulation (e.g., Data Protection Directive 95/46/EC, eCommerce Directive 2000/31/EC), although not directly binding, allow for the abstraction of national data protection implementations which may be useful for international services. Requirements with respect to the possible registration of the service and its data sets at relevant authorities, such as the national Data Protection Authorities, are explored and necessary steps for this phase are taken. Contract law and tort law have to be considered to provide input to the requirements.

The result of this phase is a set of requirements, a business plan and global architecture of the service. Management approval is required before commencing to the construction phase.

Construction. In the construction phase, the service is built, tested and deployed. This includes both developing the technical components as well as the non technical components: policies, service level agreements, contracts, procedures, institutional arrangements (with third parties), documentation, etc.

Important aspects in relation to PRIME are the adoption and integration of the prefabricated PRIME components from the PRIME toolbox into the overall system. Since PRIME relies on a credential and certification infrastructure, it is necessary to prepare, implement and populate this infrastructure with default certificates, credentials and policies. With respect to the PRIME compliance process (see below), it is also necessary to receive the required proofs for the assurance claims (for instance, privacy seals and common criteria evaluations).

All process areas need to be elaborated because they all have to be present in the operational system.

In this phase, the SLE aspects are developed in further detail. From the economic perspective, issues such as service level definition, marketing and packaging issues, brand management, customer satisfaction, pricing, education and training are developed on the operational level. The legal focus is on drafting the contracts, service level agreements with other service providers (and potentially with users), privacy policies, legal evaluation, and on formal registration with relevant authorities (privacy commissioners and law enforcement). From a social perspective, different culture/language specific implementations are developed and pre-tested with users. User tests are performed to test the user-interface and the system's functions with intended users.

Operation. The main part of the service life cycle is its operational phase. During this phase, the system is operational and all processes are involved in the processing of the (personal) data. The most important processes in the operational phase are the data and meta data processes. These will be described with respect to the operational system in more detail in sections 5.4.1.4:'Data Management Process' and 5.4.1.4:'Metadata Management Process'.

To enable the execution of these two core processes it is required to maintain the system. Maintenance, especially from a PRIME viewpoint, not only covers the technical maintenance of the system, but also organizational maintenance (such as issuing and revoking credentials and certificates, and maintaining assurance claims for system updates).

Other important processes in the operational phase that need to be mentioned here are the Compliance (including Privacy Audit as discussed in section 5.2.1) and CRM processes because they relate to guaranteeing the privacy enhanced nature of the service and the management of the relations with the users.

In the operational phase, the system has to respond to changes in the environment, including those deriving from social, economical (business) or legal factors. For instance, regulation may change, requiring the service provider to change what personal data may/has be stored and how. Also regulation, such as Basel II or Sarbanes-Oxley, may impose new requirements on the way data is handled and accounted for. Relevant economic changes may pertain to changes in the underlying business models as a result of the introduction of micro payments, or anonymous payment schemes, or an increase in income from advertisements due to rising popularity of the service. Social changes, such as increased caution of users with respect to personal data resulting from the exposure of ID fraud cases in the media, may warrant different policies with respect to personal data use in the service.

Most established businesses processes are already in the operation phase of the service life cycle. If a service provider would like to add PRIME measures to an established business process during this phase, economic assessment of a privacy solution at this phase would address both organizational and architectural feasibility. We address these in the Appendix A on this document by looking at both organizational and technical measures to address privacy concerns, directly related to the legal principle described earlier in this document This includes both technical maintenance of the system, but also organizational maintenance (such as issuing and revoking credentials and certificates, and maintaining assurance claims for system updates). From the literature [115], we note for assessment of technical viability of the privacy software solution, that end-users are concerned with observable attributes (such as Functionality, Reliability, Availability, and Efficiency). Business managers, for adoption purposes, are more concerned with Maintainability, while system administrators are concerned with Scalability, Portability, and Manageability.

For example, an assessment can include discussions of:

- Transparency: Level of awareness for both the user and the organisation of the organization's privacy policy. In the user context, how visible is the controlled authentication access to only what is needed for the business transaction.
- Maintainability: The ability to track different versions of privacy policy as changes are made. This means an examination of the firm's privacy policy and the economic impact of the transparency of such a policy.
- Scalability: For the organization, the financial and process impact of scaling the privacy solution on a wider scale than the initial implementation / application. Also the possibility of an initial deployment for one application into a larger implementation requires the appropriate economies of scale.
- Modularity: For the organization, where is the module deployed, and how application independent is the implementation for business purposes. This includes simple, consistent experience while enabling separation of contexts through multiple operators and technologies.

A major structural question with an established process or system is where in the system architecture to install technical privacy measures. In many cases, if a business service provider already has been addressing identity management (IDM) in its architecture, a privacy solution such as PRIME might be installed on top of an existing IDM framework (e.g. IBM Tivoli) where either modification or wrapping of legacy applications is not only ecomomically not viable, but at-odds with the current IDM middleware already installed, as it has already addressed the transparency issue for its own implementation. It therefore might be more cost efficient to leverage the transparency efforts of a currently existing middleware (e.g. IBM Tivoli, HP Select). The principle of data handling as a cost/obligation (D.14.2.c, page 36) to be passed on within the value chain will change the overhead costs of doing business with other parties, and maintain an obligation chain (outside of the privacy framework) that may impact the willingness of parties for adoption. As mentioned in the legal framework, the more sensitive the data, the

greater measures that need to be taken in securing its privacy. From our research (PRIME internal Deliverable F2), we see a relationship between the need for privacy and the level of information intensity in an organizational process, including organizational maturity to handle privacy along with the associated risk levels of the process. Potentially high information intensity in the value chain can be a large number of suppliers or customers with whom the company deals directly, a product requiring a large quantity of information in selling, a product line with many distinct product varieties, a product composed of many parts, a large number of steps in a company's manufacturing process, a long cycle time from the initial order to the delivered product [103].

Retirement. In the retirement phase, the system is disposed of. Decisions will have to be made with respect to how the personal data available to the service provider is to be handled. Should users be given the option of their data being transferred to another service provider, or should the data be destroyed outright? SLE factors clearly affect these choices as legal requirements, business decisions and social considerations have a bearing on what is proper termination of the service.

5.4.1.3 Components

This subsection describes the architectural components that implement the concepts defined in the life cycle model at the organisation's side and also elaborates on some basic concepts that are applied and simplify the understanding of the components. Note that the basic concepts equally apply to the user side of PRIME as they are universal in the context of PRIME. The components represent a conceptual view of what a PRIME system on the server side is composed of. The focus is on the key areas addressed by PRIME and neglects technicalities. A real deployment architecture has to take into account the business' current systems and corporate infrastructure. We start with some basic concepts of PRIME, particularly the data model and the PRIME ontology.

Data model. The data model of PRIME defines the basic semantics of data and metadata attached to the data. The data model is defined on an abstract level, that is, independent of the storage format of the data. The storage format is governed by the data schema. A prominent example for a data schema is the relational data schema that is the most widely used data scheme those days. The PRIME data model can be mapped either to a relational data schema or the proprietary PRIME data schema. The latter is more flexible, but not as performant as an appropriate relational data schema.

More concretely, the data model defines identity semantics of the data and also allows for doing automated reasoning over data using PRIME's *ontology*. The semantics is, for example, given by attaching ontology types to instance data and establishing relations between instance data items. Furthermore, the data model governs how metadata is associated to the data where metadata can be policies, the change history of attributes or their release history where the latter forms the basis of the Data Track explained later for the user side.

Various mappings between data model and data scheme are necessary to be defined when deploying PRIME-based technology within enterprise environments. An enterprise has an already deployed data model and data scheme and a mapping between those. Mostly, the data model is implied by the data schema and not given explicitly, but implicit in the data processing. When PRIME technology is going to be deployed in such a typical corporate environment, a mapping between the PRIME data model and enterprise data model needs to be established to translate instance data and metadata from one model to the other and vice versa. Furthermore, translations to the data schema, typically a relational one, are required in order to allow for using the existing data schemata or extensions thereof for accounting for further PRIME functionality.

On an abstract level, the difference between the PRIME and enterprise data model is in terms of where it is used. The enterprise data model is used for internal processing within the enterprise or a division of the enterprise, whereas the PRIME data model is used for communicating data between the enterprise and the user or between enterprises for exchanging user data.

Ontology. PRIME has defined an ontology that specifies many commonly-used ontology types for attributes and puts them in relation to each other and into an abstraction hierarchy. The

ontology is expressed using W3C's OWL which is compatible with the RDF-based data model. This allows for automated reasoning over data using the ontology as further semantics input to the reasoning process. The reasoning can be used for determining which private certificates can be used for satisfying a claim request by another party, for example by taking the abstraction hierarchy into account. Another example is for policy evaluation, again by using the abstractions defined in the ontology. An example for abstraction is to express a policy in more abstract terms, e.g., require a proof of majority age by a EU-member-state-issued electronic ID card, where the user has a German id card to use for the proof.

Data Repository. The Data Repository contains both user data and metadata. Whenever data of a user are solicited, be it personally identifying data or not, these are stored in the data repository. The agreed policy for handling the data (data handling policy) is stored as well together with an association between the data and their metadata. The data handling policy contains items like user's consent, purposes the data may be used for (e.g., an opt-in for marketing), possible recipients of the data, data retention period, and any other agreed aspects. The data handling policy is comparable to P3P [149], but can be transformed into an enforceable policy at the services side, whereas P3P typically only serves the purpose of communicating the policy to the user. Furthermore, our data handling policy is more expressive and integrates well with our access control policy framework. Data and data handling policies can be retrieved from the Data Repository by authorised components.

The organisation's policies that apply on a more general basis than data instances, are maintained in the Data Repository as well. The data handling policies and the organisation's authorisation policies together are used by the Authorisation Decision component to derive policy-based decisions.

The Data Repository, of course, supports read operations for retrieving data and metadata as required by other components and write and update operations for inserting data items or changing them.

Authorisation Decision. The Authorisation Decision component makes decisions on whether a particular access to data or a service may be granted. In addition to the access request, it uses policies provided by the Policy Management component as input. Basically, authorisations are required at the front-end system when users access services, and at the back-end system when user data is accessed for use by other components.

At the front end, whenever a user accesses a protected resource, the Authorisation Decision either allows the access (if required information on the user is available) or returns a request for claims to be made by the user (i.e. data to be provided), or denies the access. The request for data is provided in a formal language and is understood by all PRIME user client applications. The request replaces the concept of web forms for soliciting data. Instead, the user's client system displays a user interface that is independent of the organisation with which the user interacts to solicit required data.

Together with the data request (in form of the claim request), the service provider's data handling policy is also provided to the user, thus integrating data handling policies into the process. The data handling policy specifies how the recipient of claims should handle the data once released by the data subject and consists of two parts: the first part is related to access control and is enforced by the access control system of the recipient; the second part are privacy obligations, which are conditions to be met by the service provider after the access has been granted (e.g. conditions to notify users or delete data under certain circumstances), and is enforced by the life cycle data management system of the recipient. The enforcement of privacy obligations may happen related to access control decisions or be completely orthogonal to access control, as is the case for time-based data management obligations.

The data request and the service provider's data handling policy are subject to agreement with the user. A typical example is customisation of the policy such as allowing the user to opt in for direct marketing (agreeing that her personal data may be used for the purpose of direct marketing) under certain conditions.

The advantage of using the policy-driven authorisation function for deciding on the data to be requested in an interaction is that the access control policy is managed centrally on the server side, instead of being implicit within the web forms. That is, the approach is more flexible for the organisation in terms of changing the data categories to be solicited. The mechanism enables the organisation to allow for multiple different options of data sets to be provided by a user to get access to the requested resource. This will give users the choice of what claims to use in a particular interaction. Furthermore, users get a consistent user experience making their identity management easier. See section 5.4.2.3 for an elaboration of this mechanism.

Considering the component's functionality in the front end, its main task is to determine the categories of data to gather.

For the back end, the Authorisation Decision component makes decisions on access to user data by the organisation's employees or processes. An authorisation is required whenever user data is accessed for use, that is, for either processing of any kind, or for transferring it to recipients outside the organisation. This access control ensures that the risk of unintentional policy violations at the back end is decreased and thus the relevant policies are enforced. The policies that are enforced are the user-agreed data handling policies (which may also include consent for direct marketing) and the organisation's authorisation policies.

The Authorisation Decision thus realises the authorising part of the data management process and parts of the compliance processes regarding compliance with data protection legislation. Overall, the approach of automating the policy enforcement leads to cost reductions compared to achieving the same degree of policy compliance with less automated solutions requiring manual interventions.

The agreed data handling policy applies transitively for the user's data, that is, whenever the user's data held by a service provider are disclosed to a third party of from the third party to another party, and so on. In this case, the entity that wants to further disclose data regards the data handling policy agreed with the user as preferences to be enforced in the agreement on a data handling policy with the receiving entity. Such transitive disclosures can be performed to arbitrarily many entities with the effect that the newly agreed data handling policy is at least as restrictive as the user's originally customized data handling policy that also reflects the user's privacy preferences.

Federation Unit. The Federation Unit component is responsible for executing advanced federated identity management (FIM) protocols with users. FIM concerns conveying third party-endorsed claims, like attributes of users (requesters), to companies or governments (relying parties). The third party serves the role of the identity provider. Thus, the main purpose of this component is soliciting user data as governed by the front-end Authorisation Decision component. The cryptographic system we use is a private certificate system [7]. It can be seen as a generalisation of an anonymous credential system [11]. In comparison to current deployed FIM solutions, it allows for better privacy protection for the user when user's attributes are conveyed to the organisation.

In traditional FIM protocols like the Liberty Alliance protocols [14], the identity provider is typically involved in each transaction the user engages in with an organisation. This leads to higher costs for the organisation for each attribute provisioning transaction than in the PRIME solution. In addition, privacy guarantees are stronger when using our protocols as less trust is required in the identity provider by the user.

In our protocols, the user can obtain private certificates once, or renew them after months or years, and use them to make third party-endorsed claims to a relying party (organisation) without involving the identity provider in the transaction. A private certificate can be used many times by the user to make claims that are consistent with the attributes in the certificate. The certificate itself is never revealed, though.

Our approach of using private certificates allows the user to provide precisely the information requested by the organisation and nothing more. This helps realising the data minimisation paradigm. For the organisation, there is no more need to request additional data for "sanity checking" these attributes because they are third party-endorsed. Requiring only the minimally

required data from the user to provide the service, lowers the costs of data management on the server side. In the case that non-identifying attribute sets are required by the server, the data protection directive 95/46/EC would not even apply because the data would not be personal data. This would lead to further cost reductions due to lower data management requirements, while still allowing the organisation to obtain the user attributes of interest. Another key advantage of using our FIM approach is increased data quality, because users cannot make false claims due to the third party endorsement of the claims.

A leading-edge functionality of the protocols we employ is the possibility of allowing a user to be conditionally anonymous or pseudonymous. This means, the identity of the user can be uncovered by the organisation with the help of a trusted third party denoted Revocation Authority. The key novelty here is that the third party need not be involved in the transaction where a user makes conditionally anonymous claims, but is only involved in the rare case of a de-anonymisation being required. This functionality allows for anonymous service provisioning with the option of de-anonymising the transaction if the user is deviating from agreed behaviour.

The Federation Unit realises the data gathering of the organisation's data management process (see Figure 7).

In addition to the advanced identity federation protocols, the transfer of user data to other data recipients is executed by this component after positive authorisation from the Authorisation Decision component.

Life Cycle Data Management. A primary task of the Life cycle Data Management component on the server side is the management of privacy obligations. A privacy obligation defines actions to be executed on the data after data have been collected. A privacy obligation is triggered by events like access to data or time-based events. When an obligation is triggered, its set of actions is executed. Each action can be an arbitrarily complex workflow as defined in the privacy obligation. It is important to stress that privacy obligations are orthogonal to access control to data, but can be triggered by accesses to data. Privacy obligations govern large parts of the data life cycle for user data. This can, for example, encompass anonymising the data once having them in identifying form is no longer required for the business process, or their deletion. Privacy obligations comprise a sub-part of the data handling policy agreed with a user. Certain aspects of privacy obligations can be defined by the user, for instance, the obligation to be notified on the status of their data every month. We think that a Life cycle Data Management component with functionality as the one of PRIME is a key component for every server-side deployment of an identity management system as it allows for the enforcement of the privacy obligations of a user-agreed data handling policy.

Policy Management. Policy Management is used for storing and retrieving the front-end and back-end policies of an organisation. A graphical editor interacts with Policy Management for the definition and update of policies which are key activities in the policy life cycle. The component is also responsible for providing policies to other components that operate on those policies. The component is conceptually standard to any state-of-the-art system that needs policies to be defined and provided to other components.

Assurance. Assurances are claims about the data processing system of an entity, or the (legal) person operating the data processing system. Assurance claims can be uncertified statements made by the party itself, or third-party endorsed statements. The difference between those is the trustworthiness of such statements.

Assurances are either expressed by using uncertified statements as claims or by using certificates. An assurance claim can be static, as is the case for privacy seals that are issued to the organisation after a successful audit of their privacy practices. An example of static assurances are privacy seals issued by parties trusted by consumers, such as consumer protection agencies. These seals provide a certain degree of trust with respect to the audited system. They do not reflect the current state of the organisation's data processing system.

Dynamic seals can be generated in real-time by the PRIME system. These real-time-generated assurances can convey information on the current state of the system and thus complement

privacy seal-like assurances. We note that we do not think that privacy seals can be replaced by those "dynamic" seals as the further provide a third-party evaluation of the overall organisation, thus also including non-technical aspects such as the conformance to the data protection directive and the implemented processes. A proliferation of certification of companies with privacy seals and appropriate technical mechanisms as developed in PRIME can greatly help to increase user trust in companies.

A particularly interesting class of assurances addressed within the PRIME project are third-party-endorsed assurances that are created by tamper-resistant hardware chips like TPMs[43] of the organisation's data processing system. Such assurances have the flavour of third-party endorsed assurances as the tamper-resistant hardware device can be modelled as a third party that is not under full control of the organisation.[44]

An interesting part of PRIME's research is the aggregation of assurance metrics of individual platforms to assurance metrics of an overall system consisting of multiple platforms. This need not be done on a rigorous basis with any aspect of the platform to be covered, but it is a good starting point to have some key metrics for platforms that can be aggregated to metrics that are useful to describe a complete system. Typically, interesting platform metrics can be ones based on TPM technology to allow for an integrity-protected assessment. Assurances that are solely based on statements made by the platforms can be useful as well, e.g., the existence of a patched virus scanner or intrusion detection system.

Assurances, in general, help an organisation to "prove" to its users that it is going to handle user data in the agreed way and that it is using appropriate data processing machinery.

What kind of assurances can be requested is governed by assurance policies, a subclass of the access control policies protecting data.

The integrated approach of soliciting data and agreeing on a formalised data handling policy ensures that the data handling policy is, after the successful interaction, associated to the obtained user data and automatically enforced by the organisation's machinery. This integration of the handling of data and policies, and the automated enforcement, is currently missing or not consistently implemented in most systems, particularly regarding life-cycle data management. Thus, our approach helps enterprises to be compliant with their advertised policy and with important data protection provisions in EU legislation.

The components outlined above capture the key subset of the server-side functionality of PRIME's privacy-enhancing identity management. Other functionality, such as secure communication or certificate chain validation, is not mentioned here as this is already becoming a commodity and is being widely deployed.

5.4.1.4 Process Overview

The PRIME privacy management framework consists of four core processes and three supporting processes. They are described independently, but the cyclical nature of their interdepency needs.to be acknowledged.

[43] TPM is the abbreviation for "Trusted Platform Module" which is a tamper-resistant hardware device that can make statements on the software state of the machine in case the software stack supports this.

[44] These ideas are based on integrity-based computing (trusted computing). Integrity-based computing can only be utilised when the whole hardware and software stack supports these features. It is conceivable that widespread support will be available in the next few years.

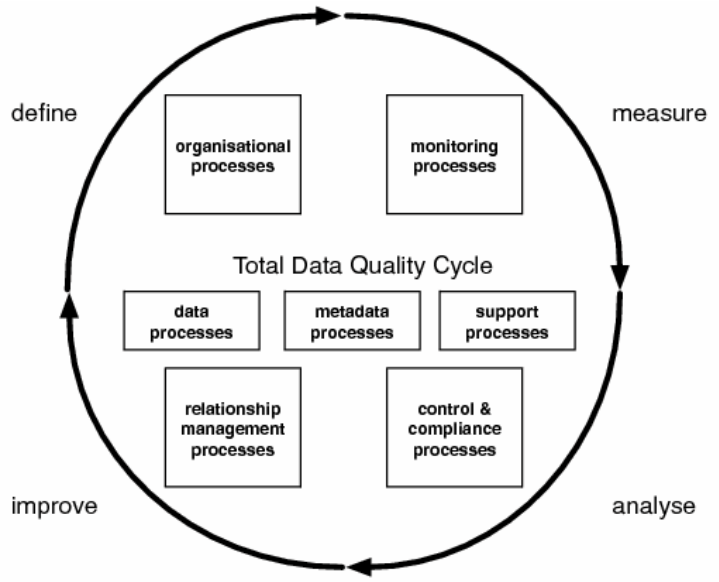

Figure 6 Top level processes in the PRIME life cycle

Organisational Processes

The organisational processes define the organisational policy regarding personal data protection. These processes entail rules and procedures for dealing with personal data. It defines roles and responsibilities within an organisation, and creates a mandate for the privacy officer in coordinating activities across different business units. Service level agreements with external organisations and operational level agreements with internal business units can be defined to manage the organisational processes systematically. Organisations can define the privacy objectives and the means of accomplishing these objectives depending on their stage of maturity, which grows with each loop of the total data quality cycle depicted in Figure 6. Concrete measures can be introduced to serve as performance indicators for the effectiveness of the privacy program. For example, the number of repeat customers, the number of users requesting opt-out, the number of incidents and complaints, are useful indicators for management to track progress towards privacy objectives.

Monitoring Processes

The monitoring process checks whether business and IT processes are in-line with the organisational privacy policy and with statutory requirements. Sensitive areas in business processes that may involve transfer of, and disclosure of, personal data can be subject to closer scrutiny. Lessons from previous incidents indicate weak points that can be prevented from recurring. Monitoring critical points in the business processes can help management to identify issues quicker, and resolve them satisfactorily before they become a public relations disaster. To support the monitoring of privacy metrics, new measures and databases may be required to provide useful reports from raw data. For example, the continuous monitoring of web pages for compliance with organisational privacy policy can reduce the number of user complaints. Privacy metrics within such a monitoring program can strive to reduce the number of incidents, as well as improve less tangible benefits such as user satisfaction levels.

Control & Compliance Processes

The control and compliance processes focus on audit and controls relevant to the business to comply with organisational policy, contractual obligations, and statutory requirements. Existing tools and techniques, such as privacy audits, provide detailed checklists for ensuring compliance.

Privacy impact assessments allow the assessment of the potential business impact of privacy incidents and the damage to business. Concrete organisational measures can be introduced to provide organisational assurance and manage the potential impact on business. The control and compliance processes facilitates the generation of audit reports for management reporting, third party assessors such as privacy seal providers, and data protection authorities. These audit reports, for example, include statements about the purposes

behind personal data collection and the intended processing of such data, allowing the level of compliance to be assessed.

Relationship Processes

Good privacy management is essential for establishing long-term relationships and user trust. Informing users and acquiring their consent can be managed through sophisticated customer relationship management systems that cater to different privacy preferences of the users/customers. Organisations that have a mature privacy program can look forward to developing closer and more intimate relationships with willing users, without offending those who prefer to maintain their private sphere. Customer centric businesses also strive to prevent privacy incidents from escalating. When incidents are reported by customers themselves, they should be rectified quickly to prevent further escalation. The relevant privacy metrics here include the number of incidents (including requests for corrections, complaints, etc), as well as more proactive measures such as number or repeat customers and the value for their transactions.

Support Processes

Respect for user privacy can be disseminated through education and awareness programs to develop a privacy sensitive culture within the organisation, as well as making sure that users are aware of the privacy policy and consent to the collection of personal data when required. Protection of personal data on IT systems also depends on IT security management in general.

Data Management Process

The data management process is one of the two core processes from a privacy point of view; the other one being the metadata management process. Although the process is primarily relevant in the operational phase of the life cycle, it is important to be aware of its structure in earlier life cycle phases to be able to implement it.

The process depicted in Figure 7 consists of the core activities that are provided by the PRIME system to process identity data. The process can be started either by receiving identity data (or related requests), or automatically if an event (e.g., time passed, policy update ...) requires it. In the first case, the identity data are gathered to be subsequently processed according to the specified purpose(s) (i.e., one or more of the processing activities are executed). Alternatively the processing activity is directly triggered by an event (e.g., a time trigger or a conditional trigger). Dependent on the subsequent process (see below) potential outcomes of the process are either failed, success, gathering (of another process instance) or deleted.

It is important to note that this process will eventually be instantiated multiple times to conduct something meaningful for the user (i.e. a use case). The Data Process uses PRIME components to establish their goals. These components may be executed on different PRIME systems like the user side (client), service provider side (server) or third party (server).

> **Example:** The data process is triggered by the user changing data locally and then choosing to update the data resulting from previous transactions that resides at multiple service providers. For each relevant service provider, this implies two process instances that are sequentially executed: The first instance on the client side starts with an event from the user which directly triggers the transferring activity. The server instance of the process receives the request via its gathering activity and processes it in the corresponding activity.]

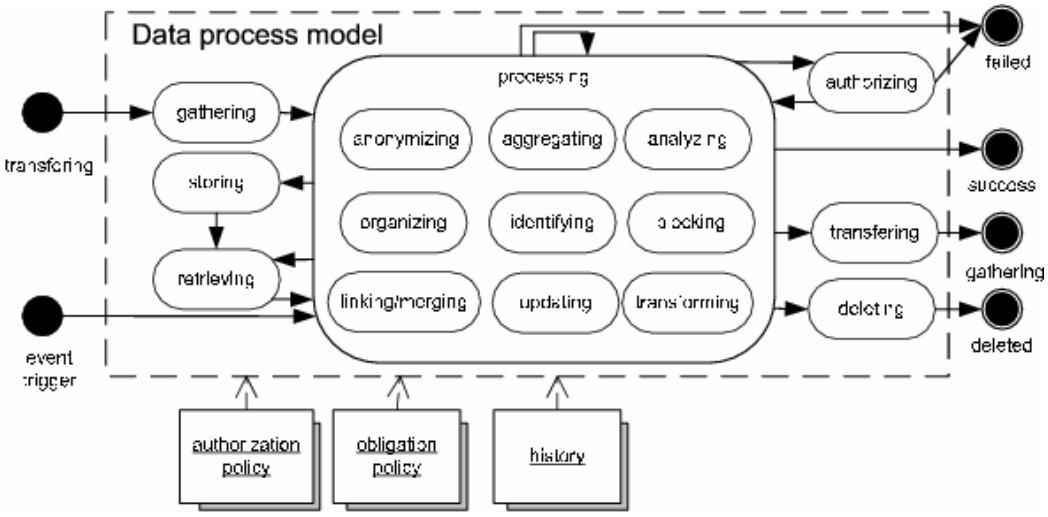

Figure 7 Data Management Process

Dependent on the purpose of calling the data process, obligation policies, authorisation policies and history are required. This information is provided by the PRIME infrastructure and is derived either from the metadata process, or from automatic system activities (e.g., logging).

It is important to note that the data process is implemented in a way that allows it to cope with changes in the environment. Ideally, it will have to be flexible and allow for changes in the runtime environment to be made without having to re-implement significant parts. These changes may be required as the result of SLE factors that may, for instance, affect the kind of personal data processed by a particular service and the way this is done. Examples are changes imposed upon the service provider by law, or changes in the attitudes of the users. Also changes in the way the business has to be run to be profitable can warrant significant changes. For instance, when a service switches from being funded by advertisement to a subscription based model, this may impact the data required for the service to be run.

Metadata Management Process

The metadata management process is the second core process (shown in Figure 8). Note that the current presentation of the process focuses on the policy part of the metadata, but other metadata handling is part of this process as well. metadata management concerns the handling of the data process. The Metadata Process manages the data handling policy. From this policy it derives authorisation policies and obligation policies. The Metadata Process also manages other metadata such as credential data (such as authentication data and certificates) and trust information. The metadata is stored persistently in the PRIME system in the Data Repository.

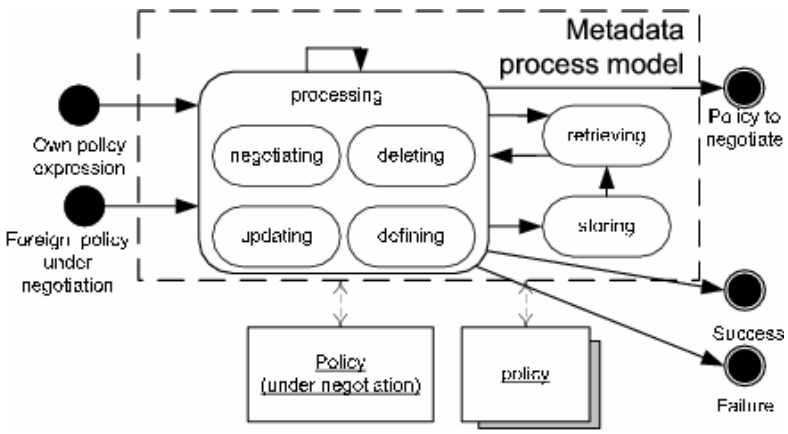

Figure 8 Meta Data Process

The process therefore provides capabilities to define, update and delete policies and other meta data (reflected in the policy expression start state of the system). The PRIME system is capable to negotiate data handling policies with a client during run time. The server will provide the client with its data handling policy when requested. The client can propose modifications to the default policy to the server which either accepts or rejects them. The negotiation can take up several rounds until either mutual agreement is reached, or one of the parties decides to terminate the process due to lack of agreement.

In contrast to the data process, no explicit gathering and transferring activities are required as those would only pipe the data through without processing them. The process terminates, dependent of the purpose of either policy negotiation or handling, with success, failure or policy to negotiate.

5.4.2 User Side

We now make a switch to the user side. We assume that users adopting the PRIME system do so because they want better control over their personal data, want to limit the risks of identity fraud, etc. They will, implicitly or explicitly, have made an assessment of socio-legal-economic aspects resulting in a decision to invest in the use of the PRIME solution.

The user side will be described similarly to the description of the server side because the primary processes of the client side mirror those of the server side. However, since the interests of service provider and client differ, we emphasize different aspects.

PRIME, from the perspective of the user, is a single application — the PRIME Console — that handles her personal data. It handles all management and disclosure of personal data for the user and is the interface to the PRIME technology. The user interface is therefore a prominent aspect of the system. Even more so, because it has to embody important parts of the functionality (e.g., informed consent has to be established through a user interface, privacy risks have to be conveyed on the screen, and so forth). We will therefore address the user interface explicitly in section 5.4.2.3.

The user side life cycle is fairly simple. The user decides, most likely on the basis of an implicit assessment of SLE considerations, to download the PRIME client side, the console and associated components. The Console requires installation and configuration and is then ready for use. During the operational phase, the user manages her personal data using the Console, discloses personal data, and checks the proper handling of her data by the various services she frequents. Finally, she explicitly gets rid of the application by uninstalling it, or stops using it. We do not need to discuss this life cycle in more detail. Instead, we focus on the user centred identity management.

5.4.2.1 User-centred Identity management (User Side Processes)

As with the service side, the user side identity management system comprises a number of processes. These are shown in Figure 9 and explained in more detail in the following section.

> **Metadata management.** Metadata management encompasses the activities related to meta-data, in particular policies, preferences, and transaction histories.
>
> Policies and preferences are typically shipped with the IDM system, that is, the definition is usually not done by the users themselves. Additionally, users may obtain their policies and preferences from trusted parties like consumer protection agencies. Only few users will define their policies and preferences themselves. This will be similar to the current situation where web browsers by most people are used as they where installed and only few people actually change settings. The reason for this is probably that it is too complicated for users and takes up too much time. It will therefore be important that the settings shipped with the IDM application provide sufficient protection for most users and are acceptable to businesses. Shipping proper policies and preferences is a key success factor for the deployment of a privacy-enhancing IDM system.

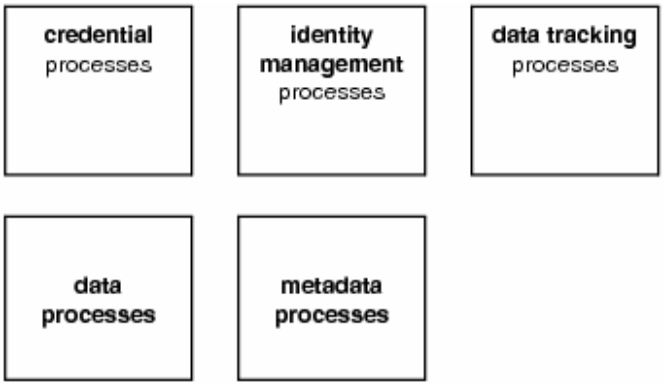

Figure 9 User side processes in a user centred identity management system

Whenever a user engages in an interaction, she will customise the data handling policy associated to the data that are being released in the interaction. This requires negotiation of the data handling policy with the provider. This involves invoking the corresponding policy negotiation process on the server side.

Note that the way policies and preferences are defined on the client side is completely different to how an organisation defines its policies. For the user-side the policy definition is intuitive and easy to handle for the average user, on the organisation side the policy definition is done by highly-skilled specialists with sophisticated policy editors. For the user side, the typical way of specifying policies is not through an explicit management action by the user, but within interactions with an organization. This concept is referred to as real-time policy definition and is particularly appropriate due to it being performed within a user interaction that takes place anyhow. However, the same activities like creation, agreement, etc., are required. The high-level life cycles are therefore quite similar.

The handling of transaction histories and update histories of attributes is captured by the metadata process as well. A prominent use of this is within the data track functionality as explained in Section 5.4.2.3.

Data Management. User-side data management concerns the management of the user's own personal data. This process mirrors the server side's Data Management process which handles obtained user data.

Creation of the data is one way data can enter the user's IDM system. Creation is done by the user entering attributes into their IDM application. Another way to create data locally is to obtain (private) certificates from identity providers an manage the associated attribute and type data. A certificate can later be used to make third party-endorsed attribute claims using the attributes in the certificate. Obtaining a certificate typically requires that the user makes identity claims to the identity provider or even obtain a certificate with traditional authentication as with a passport to obtain an electronic identity card. Note that the data management process handles any other kind of identity data that is associated to any identity federation protocol. That is, the data management is quite similar for any known federation protocol. Only the (cryptographic) protocol to perform an identity federation differs depending on the protocol we use.

Release of data is performed within transactions with companies when companies request data.

In many scenarios, there are multiple options for a user to gain access to a service provider's resource, for instance, by showing a service subscription credential, or by making a onetime ePayment. The decision which option to take, and therefore which data to release, has to be made by the user with support provided by the Identity Management Processes outlined below using the history, policies, preferences, and user input.

The data release can be done by making unendorsed claims (stating attributes), or by making third party-endorsed claims using private certificates. Different FIM approaches can be used for this. The PRIME specific version has the advantage that it uses state of the art technologies, such as

private certificate systems for asserting certified claims, policy-driven user decision support, user-side tracking of data release, a powerful access control system for companies, and assurance provisioning to the user. User side tracking of released data allows the user to investigate whether the data receiver is still compliant with the agreed data handling policy (see below).

Security Token Management. Security token management mainly encompasses obtaining and life-cycle managing security tokens such private certificates or short-lived tokens as, for example, used in the Microsoft CardSpace/Vista protocol, deciding on which tokens to use in a specific interaction, and using tokens to make third party-endorsed claims to service providers. Tokens are stored in and read from the Data Repository. Note that parts of this process are required to be executed within the Online Identity Management. Note also that this process can be seen as a specific part of the Metadata Management Process in terms of interpreting security tokens as metadata.

Online Identity Management. This process captures the interactions with other parties and its associated operations and decisions. Figure 10 presents the process in the usual graphical notation. The user gets support through the IDM application in her interaction with a service provider. The IDM application can make policy- and preferences-driven decisions, but also requires input from the user as some decisions just cannot be made automatically. Within this process, activities of other processes are required, such as reading and storing data and metadata, or releasing data.

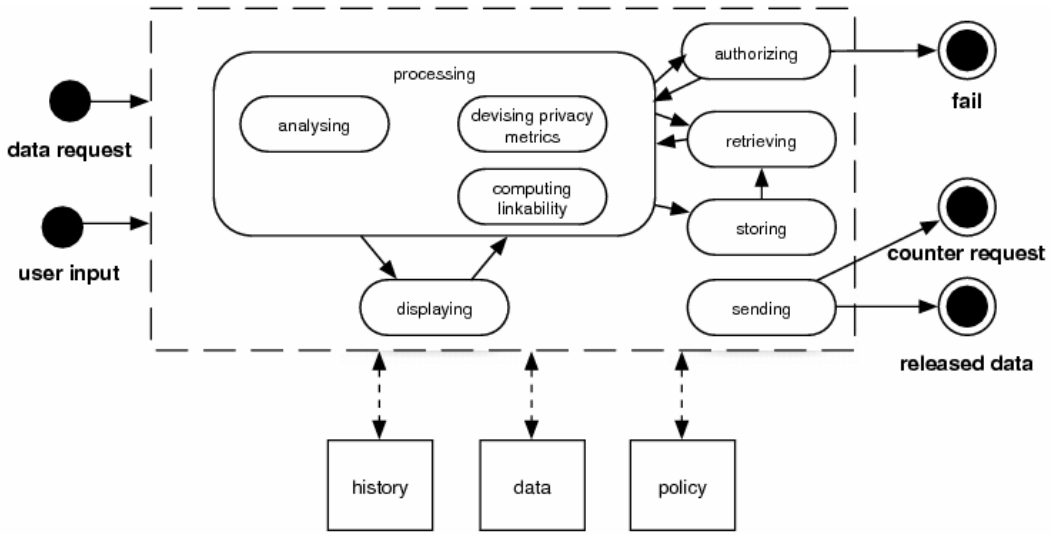

Figure 10 User side Identity Management Processes

The user side IDM application starts after a user has accessed a resource of a service provider that is protected by the organisation's access control system and requires authorisation. The server in this case returns a request for claims and its data handling policy in formalised, machine-readable form. Such a request can be a disjunction of multiple options, with the semantics that one of the options needs to be fulfilled by user's claims.

The data request is analysed by the user's IDM application. It will make a recommendation on what claims to make under which policy on the basis of the server's authorisation policy, its data handling policy, the user's data handling policy and preferences, the history metadata, the user's intentions, and the response of the user's Authorisation Decision component, and user input. This requires retrieving policies, retrieving data, retrieving transaction histories, computing the linkability of the transaction to previous transactions, devising privacy metrics for the individual options, and displaying the results to the user.

Optional step: The user's analysis can yield a *counter-request* for assurance claims (e.g. privacy seals issued to the server by parties trusted by the user, such as consumer protection agencies). Assurance claims can help the service provider to "prove" to the user that they are going to handle user data in the agreed way or that they are using appropriate data processing

machinery to manage the user data. The counter-request for claims is sent to the service provider and the service provider returns appropriate claims (such as a privacy seal). When the user receives the appropriate claims, they are analysed by her IDM system. If the analysis has an appropriate outcome, the user will release the claims initially requested by the service provider. Note that the user-side analysis is governed to a large extent by the user's *release policy*, a policy that dictates under which conditions data may be released to other parties.

An easy-to-understand representation of the data handling policy, the claims to release, the overall transaction context, the result of the assurance check, and compliance of the server's data handling with the user's own preferences is displayed to the user. A customisation of the proposed data handling policy through the user may be possible if options have been proposed by the service provider within the data handling policy. The customisation allows the user to bring their own data handling requirements into the data handling policy and can involve things like defining notification obligations in case data are transferred to third parties by the service provider, or notifications on policy enforcement, or the opt in to direct marketing. Finally, (informed) user consent is solicited for the overall transaction to be carried out.

In case of a positive authorisation decision, the actual release is performed by the Federation Unit which runs the protocols with the organisation's Federation Unit component. The transaction history is stored in the metadata store prior to data release. The user's consent, claims and the customised data handling policy are sent back to the services site, which will associate the personal data provided by the user (by the use of claims) with the negotiated (customised) policy. The whole negotiation process is illustrated in Figure 11.

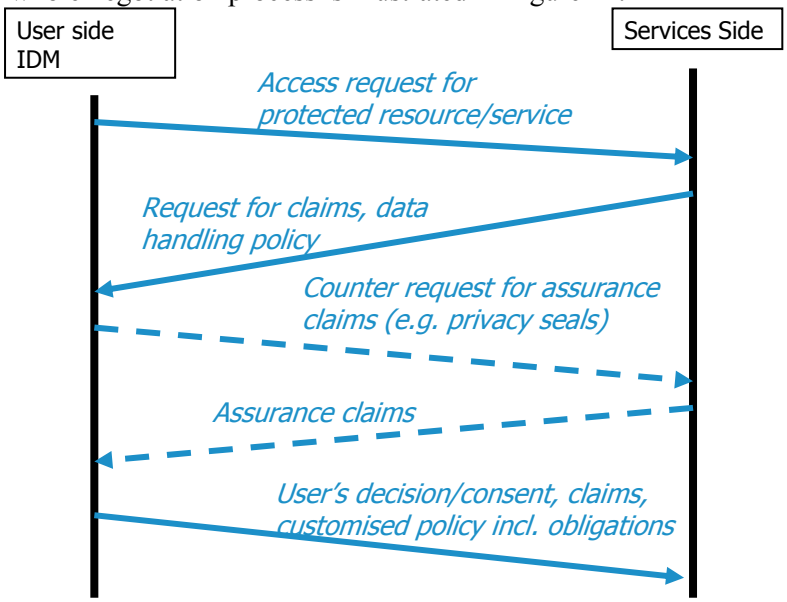

Figure 11 Data and policy exchange in PRIME (the dashed line stands for optional message flows)

The negotiated data handling policy will be enforced through the services site's authorisation engine and the life-cycle data management component.

Note that the access control policy mechanism used in PRIME is capable of doing negotiations consisting of multiple rounds in order to realize more elaborate trust negotiation semantics. Though, we think that such multi-round protocols might get too complicated for users. Clearly, more elaborate user interface techniques could weaken this argument and hide the additional complexity from the user.

Data tracking. After the user has approved data release to a server, she can use the data track functionality to obtain information on the status of her data as held by the server. This in any case includes the facility to assess which personal data is held by the organisation about the user. This aspect implements the access to data requirement of EU Data Protection Directive 95/46/EC. Furthermore, a user can request deletion, correction, and rectification of their data. Note that a request for deletion can actually result in blocking when data cannot be deleted for business or

regulatory purposes. Doing all those processes online is cost efficient for service providers, as well as convenient for the user. Furthermore, the data track function provides information about the state of the enforcement of all privacy obligations agreed between user and service provider. This means that the user can determine whether personal data have been deleted as agreed and who has received the user's data — assuming that the organisation does provide status information honestly. In case of non-compliance, the data track process can trigger further processes, for example to assist the user in filing a complaint to her data protection authority. This aspect of tracking relies heavily on the history of previously executed transactions in order to have recipient information and reference metadata (policies) for comparison. PRIME has developed used interface techniques that help the user to perform the abovementioned tasks.

5.4.2.2 Components

Next, we present, on a conceptual level, the PRIME components that implement the user side functionality.

Console. The Console, also called PRIME Console, is the user interface to the user-side identity management system. It is realised as a privileged application that accesses the PRIME middleware system. When a user engages in an interaction with a organisation that requests data, the Console displays information regarding the context of the transaction, such as the organisation's request, the proposed data handling policy, and the recommendation 'calculated' by the user's IDM application as discussed above in the IDM process.[45] The Console allows the user to customise certain aspects of the data handling policy as proposed by the organisation, such as opting in for receiving monthly statements on the status of her data held by the organisation. The creation and life cycle management of the user's policies and preferences is also handled by the Console. And finally, the Console handles soliciting consent for data disclosure within the overall process of Online Identity Management.

Because the Console is the primary tool for IDM and is used in all PRIME-enabled interactions, its user interface and user experience are of great importance. The User Interface section (5.4.2.3) provides a discussion of some of the key factors in the interface.

Authorisation Decision. This component decides on the user's access to her own data stored in her local Data Repository. It also governs decisions about access by local applications, such as the PRIME Console, and the release of data. Decisions are made on the basis of policies that are either defined by the user herself, or obtained from a trusted party like the vendor of the IDM system or by customer protection agencies, or any combination thereof. If a release of certain attributes is not allowed straight away, the component generates a request for claims, such as assurance claims, targeted at the organisation requesting the data. The data will only be provided when these requested claims are provided.[46]

Data Repository. Symmetrically to the service provider's side, there is a user-side data repository. It contains the user's own data, her policies and preferences, and the interaction history. The history mainly captures the data that have been disclosed to other parties and the data handling policies agreed with the various service providers for certain attribute data items.

Authorisation Enforcement. This component controls the flow of identity management interactions, thereby enforcing the joint decisions by the Authorisation Decision component that follows the specified policies on the one hand and the user in her interaction on the other hand.

Federation Unit. The Federation Unit on the user side executes protocols for making third party-endorsed claims to organisations, that is, for releasing third party-endorsed attributes. Currently, the focus in on using private certificates for identity federation, but the component is open for other identity federation protocols Details are explained in the server-side section of this component.

[45] See also below on ideas to involve RSS feeds on privacy and security issues in this process.
[46] The user can always override the decision of her IDM system, but this should be the exception rather than the rule.

Policy and Preferences Management. This component provides functionality for the storage and retrieval of policies and preferences and their delivery to the components using them. The component is analogous to the server-side Policy Management component.

Assurance. The user's IDM application features a component for assessing assurances provided by the service providers. It provides the associated user-side functionality to the server-side Assurance component. It deserves mention that the user-side component allows for assessing the trustworthiness of the user-side platform and communicating the status to the user or taking appropriate actions in case that the required status is not reached.

Privacy-enhancing Communication. The user's PRIME system allows for connecting anonymously to a company's PRIME system, that is, not even revealing the user's network address (typically, IP address). This is done using the onion routing, more specifically, the TOR approach[47] . In this approach, network traffic is routed over at least one intermediate hop to the destination system and only the IP address of the latest hop is revealed. This prevents the organisation from determining the IP address, though, it might still be possible for large-scale attackers, such as massively-funded governmental organisations, to obtain the network address of the user. This is an appropriate security model for PRIME, though, as PRIME's goal is privacy with respect to the companies the user does interaction with.

To conclude, it is worth noting that the architectures for a user-side and a server-side PRIME system are symmetric, although different aspects are emphasised in this document for either side due to the different kinds of users (organisation versus customer or citizen). Furthermore, it has to be noted that this symmetry has to be given up at a certain level of detail because scalability and deployment issues have to be considered. Particularly, the requirement of incorporating a server system into an existing infrastructure has to be taken into account. This may require processes to be substituted by similar provided by others.

The PRIME user side system can also be used in peer-to-peer scenarios. It this case, each user side will feature more server-side functionalities in order to handle the data of other users accordingly. We have not elaborated on this any further in this framework document as the basic ideas apply equally well regardless of whether users communicate in a peer-to-peer fashion or with organisations.

5.4.2.3 The UI to Implement Functions

An important critical success factor for PRIME will be a user-friendly and intelligible user interface that conveys and enhances trust. An important task of the user interface is also the mapping of legal privacy principles, mainly postulated by the EU Data Protection Directive 95/46/EC and ePrivacy Directive 2002/58/EC, into HCI requirements and subsequently into user interface design solutions. This will make the interface not only legally compliant, but will also give it a role in enforcing privacy legislation. A major challenge that needs to be addressed by the user interface is that PRIME is based on technical concepts and constructs, such as pseudonyms, unlinkability and credentials that are unfamiliar to many end users. The goal of realising informational self-determination[48] should ideally not involve understanding how technicalities, such as pseudonymisation, are carried out. However, when it comes to understanding the risk of being identified across different interactions with one or several service providers, some sort of notion about digital identity must be understood by the user.

This section discusses some of the issues associated to user side identity management as depicted in Figure 10. The focus will be on managing identities as part of the meta data management, disclosing personal data and managing credentials as part of the online identity management, as well as tracking personal data and gaining assurance.

Managing Identities

Even if users' real IP addresses are hidden through the use of anonymisation services and they use pseudonyms when contacting web sites, they might disclose personal attributes constituting a partial identity at some of these places. For managing their (partial) identities one could therefore imagine

[47] http://www.torproject.org/
[48] Meaning that users are able to decide how their personal data is used.

designing identity templates, allowing users to choose appropriate pseudonyms and privacy preferences depending on the service provider they contact. In PRIME, a set of predefined privacy preferences defining what types of data should be released for specific purposes under specific conditions and what is the type of pseudonymity/level of linkability to be used have been defined, from which users can choose from and which they could customize and store under a new name. This set of predefined privacy preferences includes also the most privacy-friendly options (for acting anonymously or releasing as little information as needed for the primary service).

This approach could be combined with site-specific setting for sites frequently visited, and have the user's system and service provider's systems recognise each other and re-use a previously used pseudonym (i.e. so-called relationship pseudonymity is used). This approach can be incorporated into existing web browser bookmark systems (such as Firefox' Bookmarks). A more advanced implementation could incorporate the option to remain anonymous at sites where the user is otherwise normally recognised. Figure 12 shows this approach. It offers the user regular access (clicking on the name of service) as well as alternative access (clicking on the icons) with a different privacy preference settings for these bookmarked websites. The identity management system handles the appropriate responses. The masked man symbolises a privacy preference setting with the completely anonymous interaction with a fresh pseudonym for each visit (transaction pseudonymity). This prevents the website to link the user to her previous visits (unless personal data, such as user-name and password, are explicitly given during these interactions). The partly hidden face at the IKEA bookmark invokes a privacy preference setting with the use of the previously used pseudonym for this website so that the website can see that it is a returning visitor.

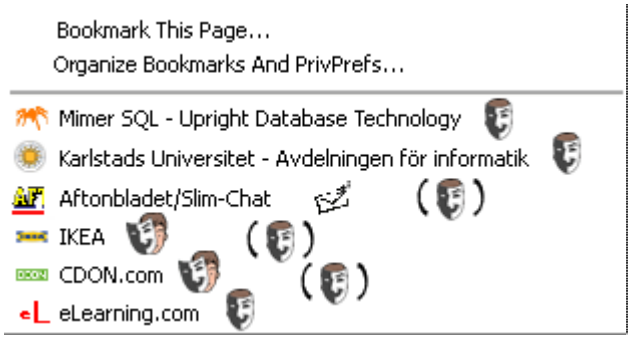

Figure 12 Bookmark list with icons for privacy preferences

The same approach of reusing or creating new pseudonyms can also be implemented in the browser's address field by incorporating multiple 'Go' buttons (see [99], or PRIME Deliverable D6.1.f).

The bookmark solution can also be used in graphical representations, for instance in the TownMap, where the user's 'Neighbourhood' represents the area (websites) where the user is more 'recognisable' than in 'Public' places (see Figure 13). Predefined areas are the Neighbourhood (where relationship pseudonymity is used by default), the Public area (where transactional pseudonymity is used by default), and the Work area (where relationship pseudonymity is used), each with different default privacy policies. This graphical approach may make pseudonyms more manageable [8], [99].

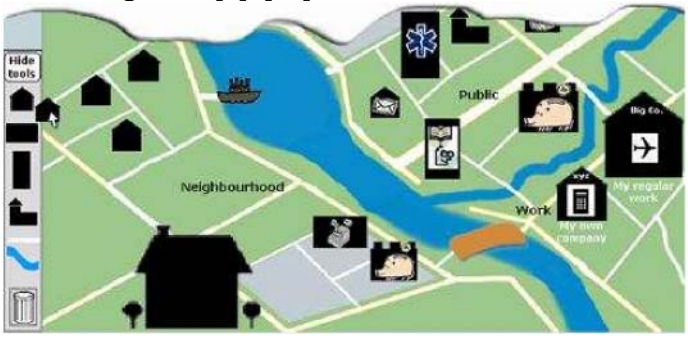

Figure 13 TownMap

Disclosing Personal Data and Managing Credentials

Irrespective of whether the user is anonymised by the use of pseudonyms, disclosure of personal data is sometimes necessary, for instance to have packages delivered home. The common legal and social requirements mentioned in 5.2.2.1, 'Information to the User', and 5.2.2.2, 'Consent of the User', apply to these situations, i.e. they need to be enforced by the respective user interfaces when personal data should be disclosed.

Instead of having all the various website data entry forms used today, with their varying ways of (and degrees of) complying with the information requirements, the PRIME Console offers a uniform way to collect personal data from the user and in the same time displaying the legally required information. The Art. 29. Data Protection Working Party recommends a "multi-layered format" to meet the requirements [4]. Each layer provides individuals the information necessary to understand their position and make decisions, but on an increasing level of detail. The top layer (layer 1) provides a short privacy notice that could be used in click-through agreements showing at least the identity of the controller and the purpose of processing and a clear indication as to how the user can access additional information by providing links to the so-called condensed (layer 2) or full privacy notice (layer 3). This multilayered approach has been used for the PRIME UI mockups of the "Send Personal Data?" dialogue click-through windows as illustrated in Figure 14 (note the the "Link to full privacy notice" where the company's privacy policy can be found). In the dialogue, the user is informed about important facts such as the identity of the data receiver, whether the receiver is within the EU jurisdiction, the purpose of the data collection, and whatever data handling policies the receiver claims to adhere to, as well as exactly what data is requested before the user is requested to agree to the data disclosure by clicking the "I agree" button. In this way, both the requirements for 'Information to the user' as well as the requirement concerning how the 'Consent of the user' is collected can be satisfied.

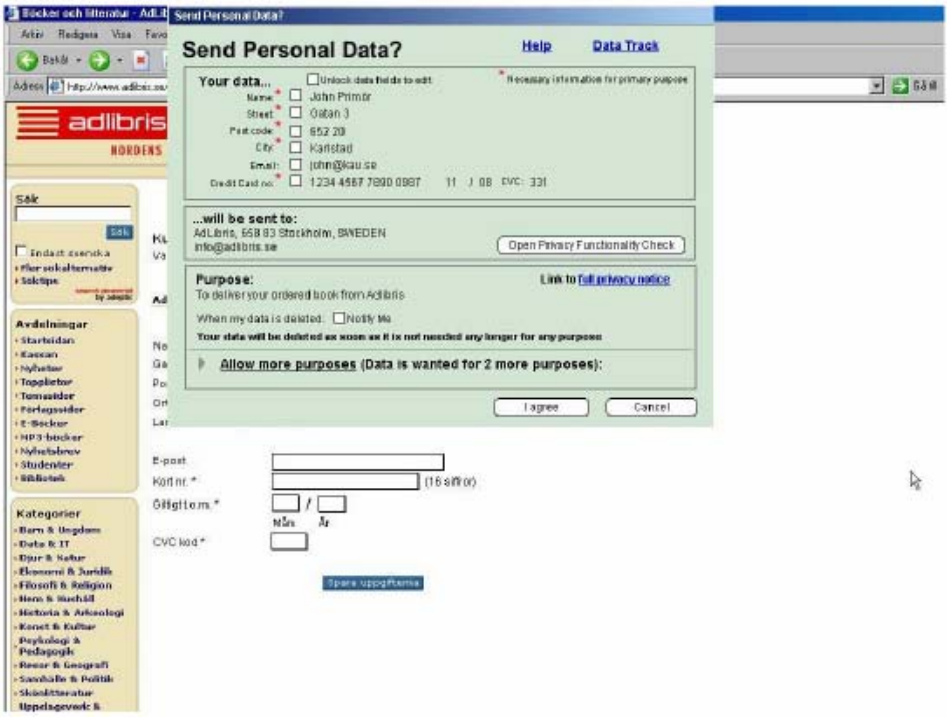

Figure 14 "Send Personal Data?" dialogue window

Moreover, the PRIME solution with one uniform dialogue "Send Personal Data?" across different websites makes it possible to harmonise the fieldnames and the layout of the data entry fields for all PRIME-enabled services. The PRIME Console interprets the data fields requested by the service provider and keeps track of what the user enters. Several 'intervening' user interfaces have been prototyped in the PRIME project to support the user in releasing data while maintaining an acceptable level of privacy. The one in Figure 14 is one example, while the one in Figure 15 represents one of the last designs developed within

PRIME – a design where it is supposed that there is a PRIME standard list telling which data types goes with which purposes (i.e., data processing purpose); this to make it possible for the PRIME system to notify the user if some data requests are excessive. (The scrollbar to the right is just a mock-up feature to indicate that the window may be vertically shorter than displayed in the figure.)

In Figure 15 the user has at some earlier point selected a pre-defined preference setting called "PRIME Profiled Shopping". This privacy preference contains a list of the (few) data processing purposes it would support, so that the "Send Personal Data?" dialogue window can notify the user if the website asks for data which are intended for data processing outside the scope of the preference setting. This is not the case in Figure 15: all three purposes are admitted by the privacy preference "PRIME Profiled Shopping", but the data type "telephone number" does not necessarily belong to the purposes of order registration and delivery, even if it is not totally unreasonably for the service provider to ask for such data for these purposes – at each instance, a "What to do" link helps the inexperienced user to decided whether she should edit the data fields or simply click the "Cancel" button.

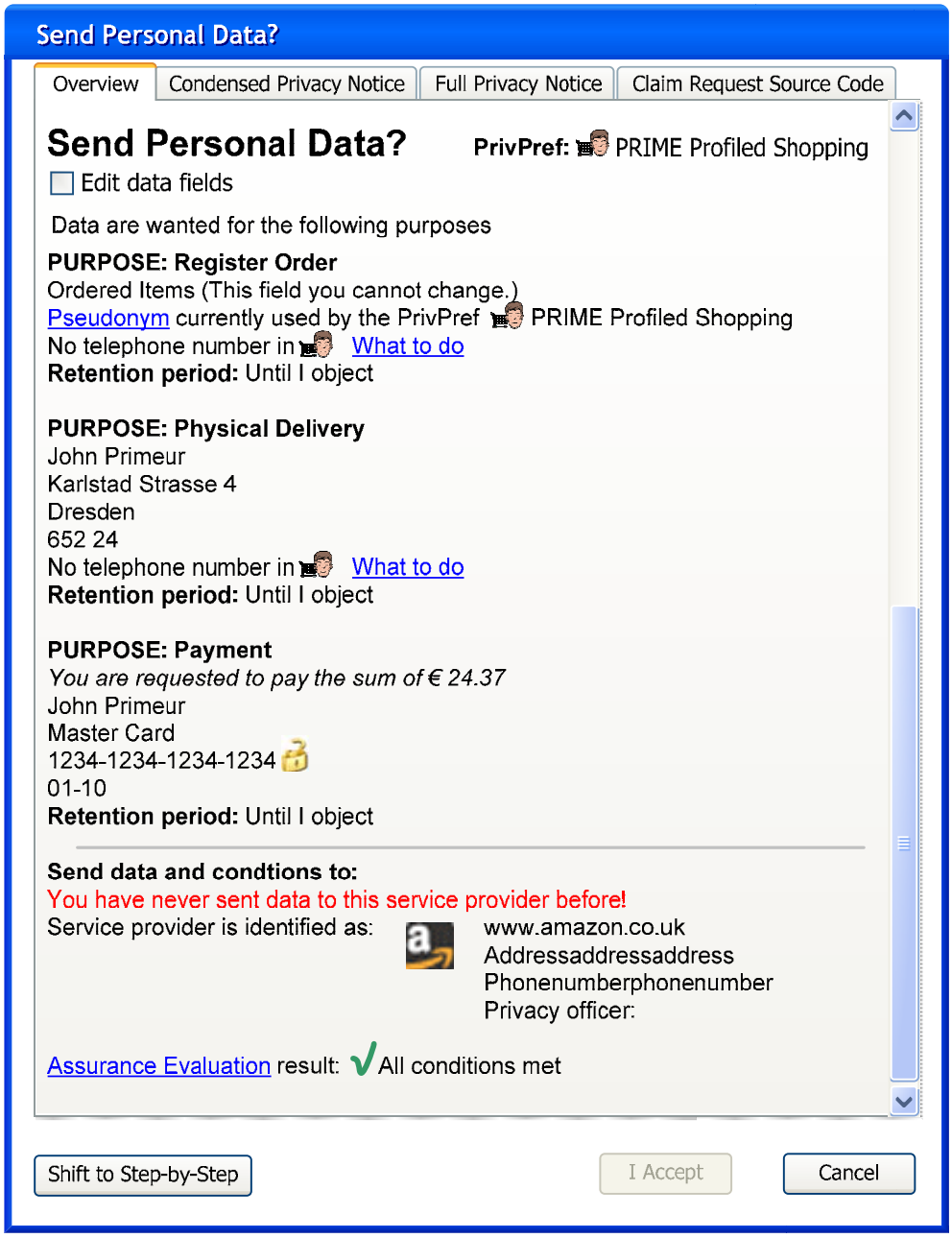

Figure 15 A purpose-sensitive "Send Personal Data?" dialogue window

An ordinary click-through window may cause users to click the "I Accept" button too easily if the preference settings have filled in all the requested data for her. Putting up "Are you really sure?" boxes does not resolve the problem as people may often click the OK button even more automatically if they have to go through an extra dialogue box every time [114]. Presenting data items in cascading menus to select data or credentials, as shown in Figure 16 has the effect that the user must read the text for making the menu choices, which means that in this case she should make more conscious selections. However, this user interface is not suitable if many data fields have to be filled; the design is intended as a special feature for very simple data requests where the user might have to select among a few credentials asserting a specific data claim. (It has not been implemented the PRIME Integrated Prototype.)

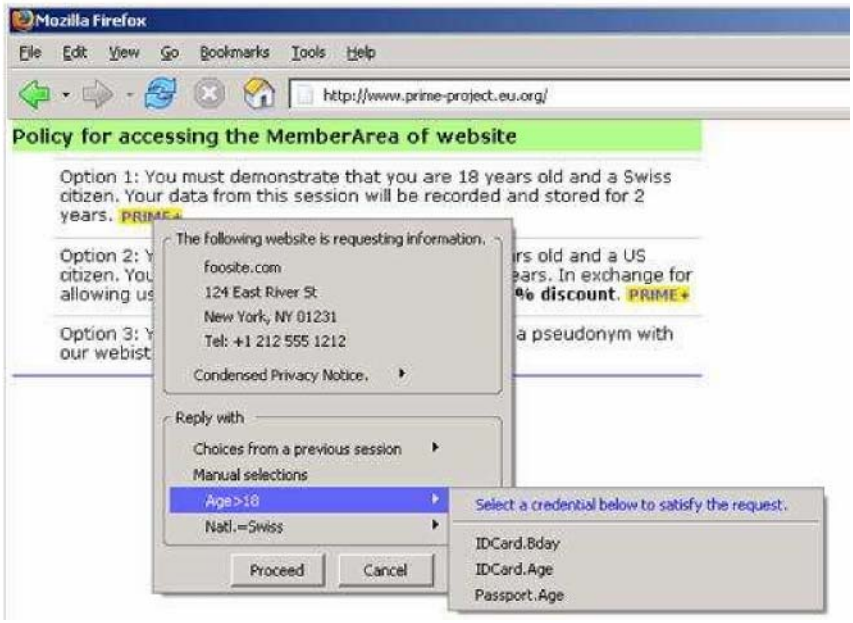

Figure 16 Menu-based Approach for selecting Credentials

"Drag-and-Drop Agreements" (DADAs) were also elaborated in PRIME as the best method for raising the consciousness about the nature of data disclosure in conjunction with the TownMap metaphor based UI design paradigm (Figure 13). Symbols were used to represent personal data – this allowed users to visibly drag-and-drop data to icons representing the receivers. Here, the user not only has to pick a set of predefined data (corresponding to clicking "I Accept" or "I Agree" in a pop-up window), but choose the right personal data symbol(s) and drop them on the right receiver symbol. These explicit actions to some extent offer a guarantee for more conscious user consent (cf. requirements in section 5.2.2.2). The PRIME Console can also use the same means to illustrate further disclosure of data among service providers.

Potentially, DADAs could be used not only in the TownMap, but also in schematic form within traditional user interfaces. A graphical representation of the user, the service provider, and third parties could then allow for direct manipulation of its individual graphical constituents. While both these forms of drag-and-drop disclosures have not been implemented within the PRIME project, one might hypothesise that they can help in alleviating one problem encountered in different usability tests, namely that a few users did not really distinguish between their computer (user side) and the Internet at large (services sides). Microsoft's Internet Explorer seems to be 'the Internet' to them, and it is not obvious to them that there is a local data repository under their control with personal data and attributes.

Tracking Personal Data

Being able to track what data was disclosed, when, and to whom, is an important feature to increase the transparency of personal data processes. Within PRIME, this history function is implemented in the Data Track. It provides the user access to transaction records, but also enables her to detect that the current use of personal data by a particular service provider is not in accordance with their joint agreement or legal requirements. PRIME usability tests have shown that people are normally not aware of their rights to rectify, erase, and block (see requirements in 5.2.2.4), and inspect (see requirements in 5.2.2.3), data

about themselves that companies and authorities have collected (these rights could however be extended as argued in [100]). The Data Track can be expanded by incorporating features that help raise user awareness in this respect and help them actively effectuate these rights and also provide them with contact addresses for help, for instance the url of the Data Protection Authorities (see Figure 17).

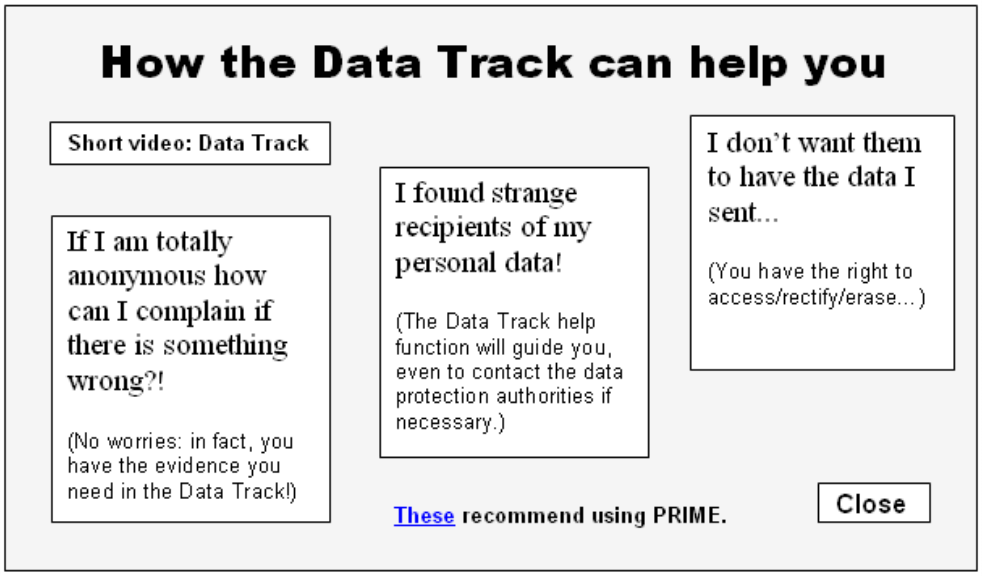

Figure 17 Four buttons for quick access to assistance functions

As people engage in many transactions, which may involve multiple providers simultaneously, the implementation of a usable Data Track is difficult from an HCI perspective. Providing users with easy tools for finding relevant records about past data disclosure is one example. In PRIME several ways have been considered: (1) Sorting step-wise by categories, such as 'Personal data' and 'Receivers'; (2) Simple search box. These first two approaches are somewhat unsatisfactory because the general user is unaware of what the system does as revealed in user tests. More suitable methods include: (3) Template sentences which put search boxes within meaningful frames: "Who has received my [drop-down list with data]?" (4) A scrollable transaction track that shows all the records at once. The records are shown in abbreviated form as small pages stacked along a timeline (see Figure 18). A slider provides the possibility to highlight an individual page in the stack. In this way, users could browse through the records without having to understand sorting or to articulate refined search requests. Obviously, this method seems more appropriate for the beginner whose amount of transaction records will be limited. For the more advanced user combinations of methods have to be explored and developed.

Trust and Assurance HCI

Another important issue where the user interface can really help to improve the whole system is trust establishment. Users have to trust the service provider and vice versa. This is an important prerequisite for user adoption (cf. section 5.2.3).Trustworthiness (of a client and services-side system) and assurance (of services-side services) can partly be communicated through the user interface. Our usability tests of PRIME early user-side prototypes and mockups, as well as other user studies [58], have shown that users often lack trust in Privacy-enhancing Identity Management, even though the technology might be perceived as usable. For approaching this problem, an interdisciplinary approach was taken in the PRIME project to investigate not only the technical options but also the social factors and HCI aspects for influencing trust (see [3]). The social factors model presented in [3] suggests that the so-called institutional layer of trust can indeed be influenced by compliance check functions that allow users to make judgments about the trustworthiness of the services side's IT system based on evidence such as privacy seals issued by trusted independent parties or reputation metrics. UI mockups for obligation management and compliance checks for verifying whether the receiving services side

still has a "good reputation", as well as a "good" privacy seal were developed and subjected to small-scale user testing (cf. PRIME deliverable D6.1.f).

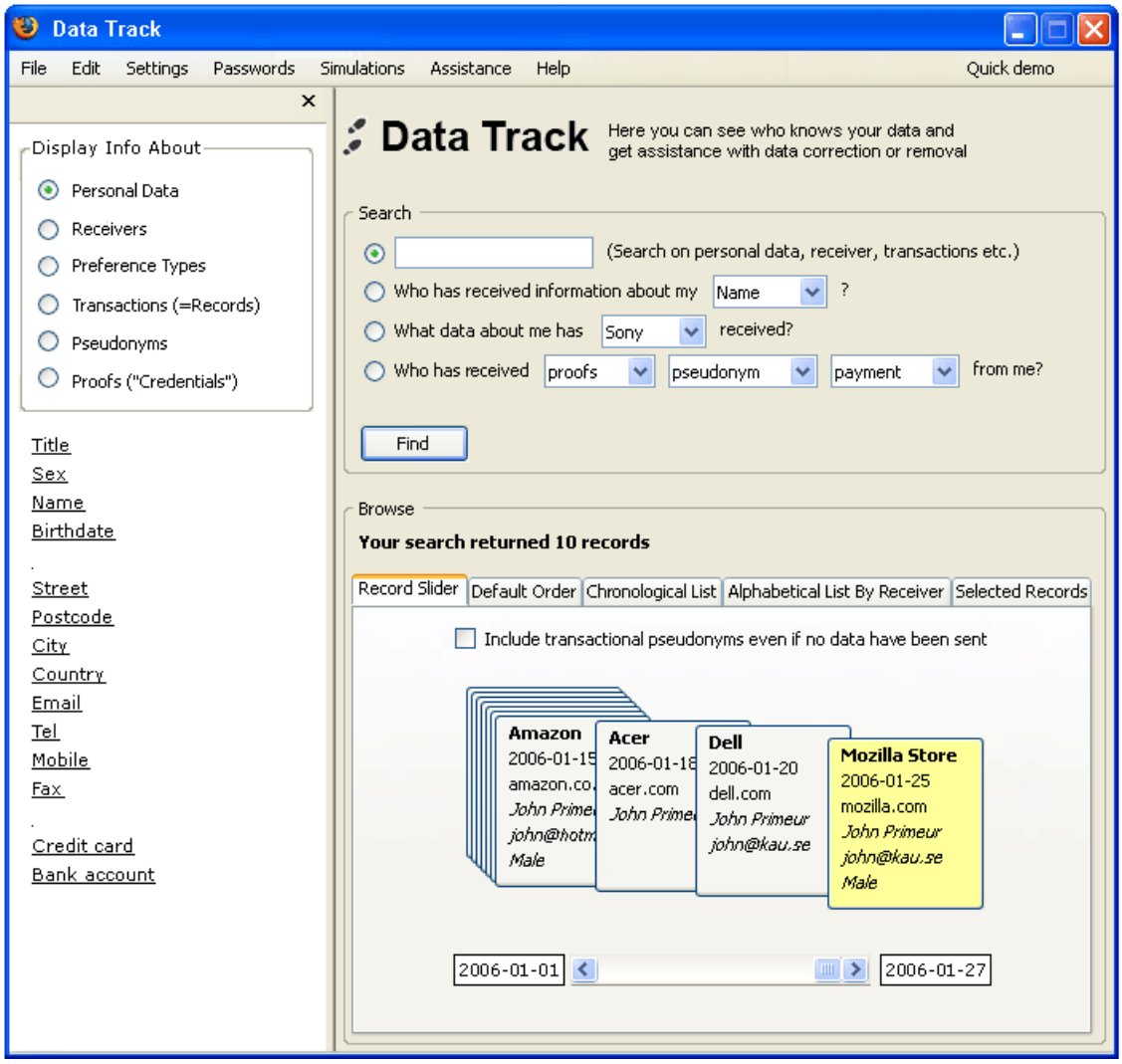

Figure 18 Data Track window including template sentences and scrollable tracks.

We also envision mechanisms for users to be informed about security and privacy incidents, especially if they might influence (re-)use of partial identities. In regard to the requirements mentioned in section 5.2.2.5, "Data Security", we think of specific information being offered by feed providers, e.g. via RSS, dealing with security and privacy information on incidents concerning protocols, applications, cryptographic algorithms, communication partners, or, indeed, any PRIME-enabled software. Users of the PRIME system could subscribe to one or multiple RSS feeds which are regularly polled by the PRIME Console. Information from the feeds which is relevant for the user is stored at the user's side and displayed: (1) when the user is going to disclose data ("Send Data" dialogue), (2) in the "Data Track" dialogue to understand potential risks related to former transactions, (3) immediately in alerting popups when the PRIME-enabled software being used is vulnerable itself. In addition if the information items contain dates when the vulnerability started and when it was discovered, this is helpful when interpreting former transactions which happened before the incident was known. Furthermore, the warnings should not only comprise mere information on the incident, but also ways how to overcome or at least deal with the vulnerability. To ensure authenticity of the provider's feed items, they are digitally signed, and the signatures are checked in the polling process. The provider's public key has to be integrated at the user's side in the feed management component which is also important to define the feeds URL and store the "trust level" assigned by the user.

5.5 Conclusion

In chapter 3 we had concluded that for effectively addressing privacy, a holistic approach is needed for developing comprehensive solutions that technically enforce strong privacy, are based on the European regulatory and legal framework, and are socially acceptable and desirable, economically exploitable, intuitive and user-friendly. This chapter presented the holistic approach that PRIME has taken to achieve this goal and its vision.

The life cycle and privacy management framework presented in this chapter has shown how PRIME components can be used in privacy-enhancing identity management incorporated in online services and what kind of decisions need to be taken into developing such a service.

The description of PRIME processes and components and their interplay described as part of the privacy management framework has also illustrated how the PRIME design principles as core part of PRIME's vision can be enforced:

- **Design must start from maximum privacy:** Initially, transactions are anonymous. Furthermore, data minimisation is technically enforced with the help of the anonymous credential system [11] implemented in PRIME.
- **Explicit privacy rules govern system usage** – Users can define their privacy preferences (i.e. data release policies) or choose from a set of predefined ones. Services sides state their data handling policies, which are presented in a form complying with the legal-socio "Information to the user" requirement (see 5.2.2.1). They can be matched against the user's preferences and can be negotiated / customised by/with the users.
- **Privacy rules must be enforced, not just stated** – The negotiated data handling policy is enforced by the services site's authorisation engine and the life-cycle data management component.
- **Privacy enforcement must be trustworthy** – PRIME forsees assurances in forms of statitc privacy seals based on privacy audits, dynamic seals generated in real-time by the PRIME system, and in future also assurances created by tamper-resistant hardware chips like TPMs of the organizations's data processing system. User interfaces for end users allow checking on the status of assurances provided by an organization and are thus important for trust establishment.
- **Users need easy and intuitive abstractions of privacy** – PRIME has researched and partially uses metaphoric representation of privacy concepts. Besides, it provides predefined privacy-friendly options for privacy preference settings which can be used or customized by the end users simplifying policy management for them. The PRIME User Interfaces are designed to meet PRIME's legal and social requirements.
- **Privacy needs an integrated approach** - Components for handling policies and for storing and handling personal data are used on both user side and services side.

Finally, the PRIME principle **"Privacy must be integrated with applications"** is addressed by PRIME through its application prototypes which will be described as a part of the next chapter.

6 Application Scenarios

This chapter will show how the PRIME design principle "Privacy must be integrated with applications" is addressed by PRIME. For this, it will be shown how the PRIME components are integrated into user side and services side tools for privacy-enhancing IDM within the application areas eShopping and LBS (Location Based Services). eShopping has been used as a demonstration scenario for the PRIME integrated prototypes. For the application area LBS, a PRIME-based application prototype has been developed.

6.1 Scenario 1: eShopping

6.1.1 Introduction

eShopping belongs to the most widely used e-applications for the Internet. In a traditional eShopping scenario, the main actors are typically the customer and the seller, (in our example an Internet shop), a payment institute (bank or credit card institute) and a delivery service. The customer visits the site of the Internet shop and inspects the offers. After the customer has decided to purchase something in the Internet shop, she places an order. Generally, this order contains not only the declaration about the purchased items, but also the name of the customer and address information for the purpose of delivery. The customer usually needs to give the seller also her credit card number or state that she pays in advance by bank transfer or check. The customer may submit special sub-attributes, e.g., vouchers, trading stamps or her customer ID for special discounts; the seller may also ask for an age verification, etc., in particular situations.

Both the seller and the customer have an interest in the other party fulfilling its obligations, i.e., that the seller sends the ordered goods and the customer pays the price as agreed upon. If there were business connections before, the gained reputation influences the current transaction. The seller's reputation is also influenced by a professional and respectable appearance or other customers' experiences.

The customer typically either asks her bank to transfer the purchase price to the seller's account, or she uses her credit card. Often, credit card payments are the only supported payment method. If the customer uses her credit card, she gives her credit card number, the valid date and name to the seller. The seller asks the credit card company to remit the money and the company will do so if the data check yields positive results. The currently most popular way of delivery of purchased products is via a shipping provider, who for this purpose receives the customer's name and address from the Internet shop.

6.1.2 Privacy Risks

A drawback of all of these personalised services is that the customer's habits and preferences reveal intimate details that not everyone may want to share. In a classical eShopping scenario, data about the customer's shopping habits and interests are exposed at the seller's and the payment institutes' sides. For instance in an online book and movie store, sensitive information about what types of books or movies (e.g. light literature or light comedies, books or reportages about specific deseases, horror movies, specific man slayer movies, pornographic movies, political or medical documentaries on specific topics) a customer is looking for and is purchasing, could be stored and used for extensive consumer profiling, which could possible be shared with other sites. Such consumer profiles may allow the store, at least in theory, to speculate or to derive conclusions about the political opinions or health or sex life of a consumer, i.e. information that classify as special categories of data according to Art. 8 of the EU Data Protection Directive. Most customers have practically little insight and control over these data processing practices, but one may expect that people may increasingly worry about these practices.

Whenever the customer needs to provide some form of assertion or authorisation or certificate, she has to send a copy by mail, fax it or present it physically, which is cumbersome. The degree of anonymity is very low, especially if assertions, authorisations or certificates are involved.

6.1.3 Privacy Requirements

A PRIME-based solution for eShopping applications has to fulfil the legal, social and economic PRIME requirements as summarised in section 5.2.

Special attention needs to be paid to the principle of data minimisation. In particular, the customer's data and pseudonyms should be linked only when necessary or when she agrees to it, i.e. the phases of browsing, of seeking for advice, of choosing the product, of payment, and of delivery should be separated as far as possible. This will also minimise the risk of profiling. Usually there is no need for the Internet shop to ask for the customer's address or payment information, which would then also allow the shop to uniquely identify the customer. Instead the eShopping business process can be divided into the three separate parts Order, Payment and Shipping, where every involved party receives only the data needed for their purposes directly from the customer. This means that the Internet shop only receives information about the placed order, the payment provider (credit card company) receives the payment details and the shipping provider receives address information directly from the customer (see also [9]). Such separation of processes on the need to know basis for enhancing the users' privacy has been proposed also in academic concepts (e.g., [19], [21], [101], [21]), as well as in practical specifications such as the Secure Electronic Transaction standard [122]. Nonetheless, preferably procedures for anymoumous payment and delivery should be provided.

The design of a PRIME-enabled Internet shop should also be flexible enough to deal with differences in the perception of privacy and trust in different social groups and EU member states. Differences might occur in perceptions about what constitutes privacy sensitive information, age restrictions on content, preferred payment methods and trust increasing institutions..

6.1.4 Outline of a PRIME-based Solution

We now outline a PRIME-based eShopping solution, which is also illustrated in Figure 19. The PRIME Console will be used for the IDM interaction with the Internet shop. By utilising PRIME's anonymous communication component and the private certificate system of PRIME's Federation Unit, all activities within these phases can remain unlinkable from each other and only the information requested by the Interent shop is released and nothing more. Hence, the privacy principle of data minimisation is enforced with respect to the transaction. Besides, as described in section 5.4.1.3, the private credential system used in PRIME allows for conditionally anonymous or pseudonymous users, i.e. in case of misuse, the identity of the user can be revealed with the help of a Trusted Revocation Authority. PRIME's data track functions help to enforce the privacy principle of transparency with respect to the data involved in the transaction.

In the following, the PRIME user-side processes online identity management and data tracking of the privacy-enhanced PrimeMovieStore scenario are described.

User Centred Online Identity Management

The Online identity management process (cf. section 5.4.2.1) of the privacy-enhanced scenario can be divided into the phases browsing, negotiation and purchase, payment and delivery as described below.

Browsing

The customer browses the Internet shop's web site anonymously. There is no need to provide any customer identity data or Internet address within the browsing phase. If a customer participates in the shop's loyalty programme or wants to receive personalised advice, she can show a proper credential without revealing any other personal information; this should be sufficient for taking part in the programme or receiving personalised advice.

Negotiation and Purchase

Also for the actual purchase of items, it is actually sufficient that the customer uses pseudonyms for communicating with the Internet shop. In case that the merchant requires to know certain properties of the customer (e.g., whether she is over a certain age, for which a film has been passed or which she

must have in order to conclude a contract), her PRIME IDM application can prove this without releasing identifying information by using PRIME's private certificate system. A new transaction pseudonym can be used for each purchase, such that individual purchase transactions remain unlinkable to the others and unlinkable to the browsing phase. If reputation in the eyes of the shop is to be built up, the same relationship pseudonym can be reused every time the customer gets in contact with a specific shop. This still prevents linkage of the customer's profile with her profiles at other merchants.

Nevertheless, according to current business practices, the store may request further personal data from the customer, e.g. for the purposes of delivery and payment (e.g., name, credit card details). Together with the data request, the Online Store's data handling policy is provided to the user, which is subject to agreement with the user. The user has the possibility to customise this policy, for instance, by allowing the use of her personal data for additional purposes, such as direct marketing for receiving special offers, and/or dictating privacy obligations, for instance for being regularly notified about the status of her data. Before releasing any personal data, the user's IDM application can check (anonymously, if desired) that the services side (Internet shop) complies with the user's preferences, including trust requirements. Depending on the user-related data being requested, the user's system can request assurance claims from the Online Store such as proofs of the Internet shop's platform properties, privacy seals issued by Data Protection Commissioners or reputation metrics. Once the Internet shop has provided the assurance claims as evidence for trustworthiness, the user's access control has accepted them as sufficient, agreement on a data handling policy could be established, and user's consent is given using the Console, the requested data are disclosed to theInternet shop.

Payment

The payment might be performed by means of credit card, mediated by a PayPal, card processor and a bank, or by means of anonymous eCoins, based on PRIME's anonymous credential system that are sent directly to theInternet shop. The use of eCoins is preferable from a privacy standpoint because it prevents any linkages between payment and purchase due to the unlinkability properties of credential transactions.

If payment is done via credit card, the customer's credit card details should preferably not be requested by the shop, but directly by the credit card institute. For this purpose, the shop would send to the user the price information and a transaction-ID for the purchase transaction. The customer's IDM system would then contact a credit card institute of the customer's choice, which would request the credit card details and subsequently inform the shop that the payment for the purchase transaction-ID has been completed (see [9] for details).

Delivery

Digital goods can be downloaded anonymously.

If a delivery service is used to deliver tangible goods, the customer's IDM system should, similarly as described above for the payment procedure, send her address details directly to the delivery service. The customer's personal address is then only known to the delivery service, while the content of the goods being delivered is only known to the shop. In PRIME, a UI wizard has been developed to guide the users through such multi-party transactions involving the shop, a payment institute and a delivery service (see [9]).

If the customer does not wish to disclose her personal address at all, a pick-up point could be used, such as a 24/7 gasoline station, from which the goods can be fetched.

Data Tracking

If personal data has been released to the Internet shop by the user in either identifiable or pseudonymous form, she can use the data track function to obtain information about the status of her data. In particular, she can use the Data Track functions provided by the PRIME Console to access her data, to check the fulfillment of agreed privacy obligations, or to request to delete or block her data if the current processing of her data does not comply with the agreed data handling policy or with legal privacy provisions, or if she simply wants to revoke her consent for the further usage of her data, for example for direct marketing.

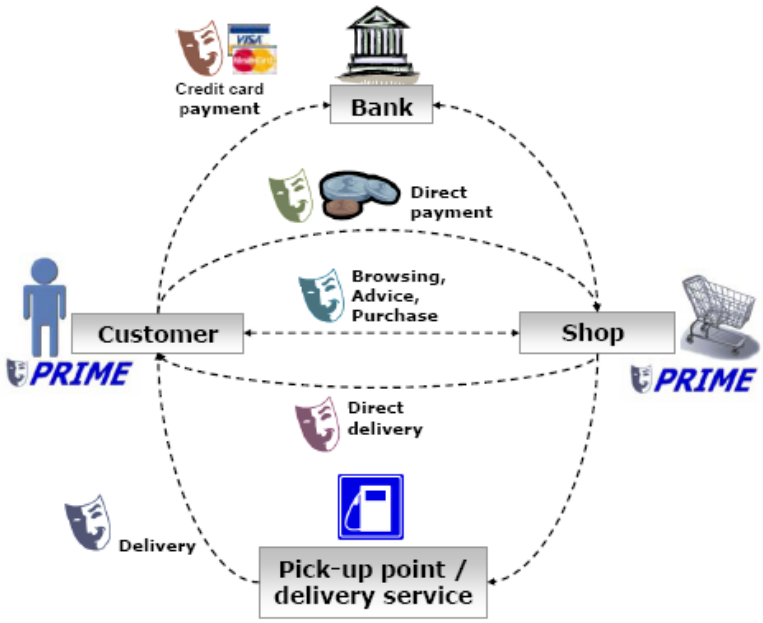

Figure 19 Privacy-enhancing eShopping in PRIME

6.1.5 Conclusions

In the example presented here, the design started from maximum privacy and maximum flexibility for the users. The end users can choose and control whether they act (browse, shop) anonymously, pseudonymously or whether they release personal data under specified privacy and trust policies. Hence, the privacy principle of data minimisation is enforced for the browsing and transaction phases. The authorisation decision component at the Internet shop's side enforces the customer-agreed data handling policies, and particularly enforces the legal principle of purpose limitation. Assurance claims, such as third-party endorsed statements, can help companies to prove that the policy enforcement will be "trustworthy". Furthermore, as pointed out above, the data track functions make the data processing transparent to the users, and allow them to exercise their basic rights.

This scenario does not only illustrate that PRIME enhances privacy for its end users. The example also shows that PRIME applications still allows companies such as the Internet shop to conduct their legitimate business interests or activities, such as the ones listed in section 3.4.2, with less or no personal information. Reasons for businesses for collecting personal data such as to better serve their customers, to develop better services and products, to recognise returning customers, and/or to be able to conduct targeted or personalised marketing can also be well achieved by the use of relationship pseudonyms. Companies could offer special bonus programmes, special awards or direct marketing offers to returning customers. Also (financial) risks can be mitigated, because PRIME's (private) certificate system allows customers to prove certain attributes, such having passed an age limit, e.g. to conduct legally binding contracts, without revealing their exact age or any other personal details.

Finally, also defaulting customers (for instance customers that do not pay, or users that distribute copyrighted watermarked content) can be addressed. Users can also be addressed in the case that the payment process fails, or when law enforcement requires this. If anonymous eCoins, based on PRIME's anonymous credential system, are used for payments, the identity of the paying customer could still be revealed with the help of a trusted Revocation authority.

6.2 Scenario 2: LBS

6.2.1 Introduction

Location based services (LBS) is an innovative application area that is under rapid development. When using LBS applications, information about the location of the user (or more specifically, the user's device) is passed to the service provider to offer the user a value-added service, as illustrated in Figure

20. Since location information is considered sensitive by most users, a main challenge will be to ensure that the user knows, decides and controls to whom location information and other personal data are disclosed.

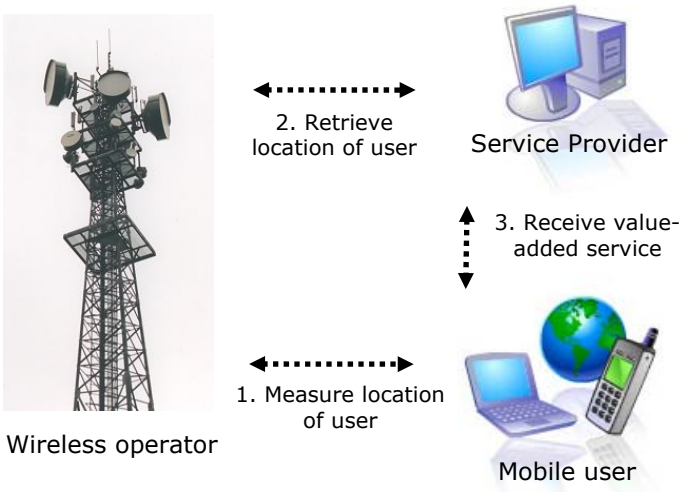

Figure 20 A generic LBS application

The mobile Internet applications differ from general Internet applications mainly in two aspects:

Mobility of the user and terminal: A user / terminal accesses services from a variety of networks with changing device and network parameters and possible periods of no connectivity;

Location sensitivity: Applications can process location information to add value to an application.

The location is either measured by the device itself using specialised hardware, for example by beacons or GPS (General Position System) receivers, or by the mobile operator in the operator's domain. For mobile phones, the latter approach is still the most common. However, Bluetooth GPS receivers are currently becoming more and more widespread. These wireless GPS receivers are small battery driven devices which are easy to connect to devices such as mobile phones, PDAs or laptops.

Important roles in an LBS scenario include:

LBS user: This is a user that is willing to disclose location information in return for an added value service;

Location Provider: A location provider is the source of information about the location of the user. The mobile operators often also act as location providers or, if the user's device has location measuring capabilities, the user can also act as the location provider;

Mobile Operator: Among other things, the mobile operators are controlling the technical infrastructure of the wireless network over which the communication between the user and the LBS provider are taking place;

LBS Provider: This is the entity that offers the LBS applications to the users. To provide a user with a location based service, the LBS provider retrieves the user's location from the location provider. The LBS provider may be the same organisation as the mobile operator;

Location Intermediary: This is an entity that controls the dissemination of detailed information about the user's location, and provides useful context information to interested LBS providers. A detailed log about what information that has been disseminated to whom is kept, which can later be scrutinised by the user.

When a mobile operator is acting as the location provider, the user has little or no control over how the information about the location is transferred to the LBS provider. Today, the only available option for totally preventing the possibility to be localised is to turn off the mobile device. This situation is more

problematic from a privacy perspective. However, if instead the user acts as a location provider, the handling of location information becomes more transparent, since now the mobile device itself is responsible for both measuring and releasing the location information.

In our PRIME-based solutions we generally assume that the LBS provider and the mobile operator are separate organisations. However, as mentioned above the mobile operator and the LBS provider may be the same organisation. This situation is further exacerbated by companies that try to monopolise location information obtained from GPS devices by using proprietary interfaces and encryption technology. The problem when mobile operators develop and deploy LBS applications themselves is that since the mobile operator both owns and operates many different LBS applications, and further controls the collection of the location information, she can potentially aggregate vast amounts of personal data into extensive customer profiles.

LBS applications can be divided into single-user applications and multi-user applications (also called peer-to-peer applications). In single-user applications there is a direct relationship between the user and the LBS provider, and the user does not directly interact with other users. In contrast, in multi-user applications the users communicate directly with each other, while the role of the LBS provider is mainly to assist the users in establishing these relationships with each other.

LBS applications can also be divided into applications where the user either explicitly "pulls" the information from the LBS provider (e.g. by explicitly sending her location) and applications where information is automatically "pushed" to the user by the LBS provider. Since in the second approach the LBS provider is automatically re-positioning the user at regular intervals, the latter kind of application is also characterised as position-tracking or location-aware applications.

LBS applications operate in a complex environment with different stakeholders. Moreover, these services need to cope with many legal and business requirements, including the additional cost of localisation, and the adherence to privacy laws. In particular, the abovementioned push-services are difficult to implement, since on the one hand many business models for selling information about location currently charge a fixed amount per localisation. Since push-services are regularly re-positioning the user, such a cost model is inappropriate for such services, if not the cost per localisation is very low. Also positioning-tracking LBS application generally causes much higher privacy concerns.

One important dimension that has to be considered for LBS applications regarding the technical environment is user mobility among the LBS / M-Commerce infrastructure. That is, users of mobile applications should be able to "roam" from one particular network access point to another. Also, they should be able to "roam" from one LBS provider to another. On top of this, they re-use applications or use applications for the first time.

Table 3 – A classification of the LBS applications.

	Pull LBS	**Push LBS**
Single-user LBS	Finding Location and Guiding	Mobile Commerce Disaster Management
Multi-user LBS	-	Person Finder Mobile Dating

6.2.2 LBS Applications

Some typical and useful LBS applications that are already developed or offered today are summarised in the following list and are classified in Table 3 according to single user/multi user and pull/push LBS:

- **City Guide:** These are LBS applications that are also called "find the nearest" services. They allow tourists that arrive to a foreign place to use a mobile device to retrieve information about nearby restaurants, hotels, exhibitions, pharmacies, cinema programmes, nearest taxi stands and much more.

- **Travel Navigation:** When driving from one location to another, the mobile user can receive information about routing and the traffic situation in the whereabouts. For example, if there is a traffic jam in the close proximity of the user, or if the user is approaching a very slippery portion of the road, he/she can be notified.
- **Friend Finder:** In the traditional Internet, so called "buddy lists", such as ICQ or MSN Messenger, are popular services. These kinds of services (often called "friend finders") are have appeared in the mobile world, now including the users' physical locations as an additional parameter. By using a friend finder, a user can keep a list of her friends together with an indication of their current location.
- **Child Control:** These are a special kind of commercial person-finder LBS application. Parents can subscribe to such LBS, which provide them with the current location of their children and alerts them, e.g. when the child enters or leaves an area as programmed by the parents.
- **Mobile Dating:** Mobile dating with localisation enables partner search in the area in which a person is currently located. User profiles are stored with the service, and whenever a person seeks company, the dating LBS looks for matching profiles in her close proximity.
- **Mobile Marketing:** Mobile marketing and couponing services target individuals to be able to provide the user with personalised advertising, offers and coupons. In contrast to classic advertising and online marketing on the Internet, mobile marketing knows an individual's profile as well as the location, and both data sets are used to sell marketing opportunities to businesses.
- **Disaster Management:** These are eGovernment applications that are under discussion and in development. In the event of a disaster, a disaster manager could be used to localise mobile phones in certain areas of the surrounding areas of the disaster to help evacuation planning. The individuals who are closest to the danger can be informed first and selectively to avoid traffic jams and panic. Individuals could also receive disaster warnings for the area in which they are currently located, for their property when they are away from home, or for members of their families when in separate locations.

6.2.3 Privacy Risks in LBS Scenarios

6.2.3.1 Informational Privacy Risks

If proper security and privacy measures are lacking, the LBS applications described in the previous section could be misused. Major threats caused by location based services to the user's right of informational self-determination are unsolicited profiling, location tracking and the disclosure of the user's social network.

Personal data such as location data, the user's preferences, business activities and the kind of information that a user requested could be compiled and stored by service providers in detailed user profiles. Location data also reveals information about the user's current context, e.g. whether she is currently at a political ralley, casino or sport club. Push LBS often require to some extends user profiling in order to provide adequate information, and are for this reason especially challenging for privacy. Examples of potential misuse scenarios of such profiles could be unwanted marketing, digging in the past, blackmailing politicians etc.

Location data could also be misused for unsolicited location tracking by misusing the information about the movements of mobile users. If the location information is not properly protected, persons could be tracked for the purpose of robbery, kidnapping or looting. If service providers cooperate with other service providers or network operators and they merge their data sources, the problems related to profiling and tracking may be further intensified.

Another problem is that exposed information about social contacts can be revealed that is often of a private nature. In a misuse scenario, a list of the close friends and private locations of a user can be gathered by an unauthorised party. These privacy problems described above are especially an issue for multi-user LBS scenarios, such as friend finder.

6.2.3.2 Spatial Privacy Risks

Another problem is that the user's spatial privacy, i.e. the user's possibility to control what is presented to her senses, is affected by SPAM and a lack of efficient reachability management. Marketing information is of great value to spammers and, as in the traditional Internet, the obvious risk is that spammers will send unsolicited emails to persons with matching profiles.

For today's commercial multi-user LBS applications, such as friend finder, the user lacks efficient control over her reachability. For friend finder applications, a user can turn off the possibility to be localised and thus become "invisible" if she does not wish her friends to know her location. When a user is invisible, she cannot be localised by any of her friends. However, it is usually neither possible with today's commercial LBS applications for a user to select visibility for a subset of friends in her friend list, making her reachable by this subset of friends and unreachable by others, nor is it possible for a user to configure her reachability on the subject matter.

6.2.4 Privacy Requirements in the LBS Scenarios

Also for LBS applications, a PRIME-based solution has to fulfill the legal, social and economic requirements as summarised in section 5.2. In this section, we further elaborate specific privacy requirements for LBS. The requirements for the different LBS scenarios have been divided into general PIM requirements, which are shared by all LBS scenarios and PIM requirements that are specific to one or some of the scenarios.

6.2.4.1 General Privacy Requirements in LBS Scenarios

The users of a PRIME-based LBS application should have the possibility to set their privacy preferences on "per service" basis. This means that different settings could apply for different services. The principles of data minimisation and avoidance should be followed, i.e. it should not be possible for LBS providers to collect more data than necessary and the data should not be kept longer than necessary. Services where the current position but no directly identifying data are needed should be provided anonymously if a user desires to be anonymous. In these cases, the user must have the possibility to pay for the service using an anonymous payment scheme.

In Table 4 below follows a table with a summary of general PIM requirements present in all of the LBS scenarios earlier described.

Table 4 – General privacy requirements for a PRIME-based solution.

Requirement	Textual description
Either informed consent or anonymisation	LBS can only be activated by the users, and data is only collected with the users' informed consent or if location data is used anonymously. Also, according to Article 9(I) EU Directive 2002/58/EC [36], the user have the right to temporarily refuse processing of location data even if consent was obtained, as well as the right to withdraw her consent for the processing of location data at any time
Flexible preferences	The users must also have the possibility to set their privacy preferences in a flexible way, e.g. depending on the service provider, the providers policies, etc
Data minimisation and avoidance	The principles of data minimisation and avoidance has to be followed by LBS providers
Anonymity towards 3rd party LBS providers	By default, users should be anonymous towards a third party LBS provider if the identities of the users are not needed for providing the service
Unlinkability of user data	User-related data used by different third party LBS providers should not be linkable, unless explicitly desired by the user
Anonymous	Anonymous payment should be possible, e.g. by the means of eCoins

payment	or anonymous bank transactions
Transparency in data collection	Transparency for users and no hidden data collection or processing
Proof of consent	To aid the users in enforcing their policies, they must be provided with proof of the consent they gave to the LBS providers.
Data track functionalities	The users should have the right to access their location data on the service side and further be able to use data track functionalities to see the history of their data
Management of user data	The users must be able to manage their identities, pseudonyms and other identifiable information, in particular in relation to their mobile phone numbers
Policy management	The users must have the possibility to configure which profiling and context data for what purposes and under which conditions it is stored, and used
Flexible authorisation schemes	The policies must permit for flexible authorisation schemes, such that application providers can implement authorisation methods as single sign on in virtual domains, etc., without restrictions from PRIME
Legacy integration	The architecture must integrate well into existing infrastructure
Privacy protection dispute resolution	In case of a dispute it must be possible to access resolving information in the most privacy protecting way possible
Specify policies for push information	For the push scenarios, the user must be able to configure with a fine granularity the conditions (regularity of positioning, purpose, etc.) under which she allow what kind of push information to be sent to her. She also must be able to set complex disclosure policies on one of the service providers hosts

6.2.4.2 Application-specific Privacy Requirements

This section discusses application specific PIM requirements for the different LBS applications described in section 6.2.2:

Finding Location and Guiding scenario: In a PRIME-based finding location service, the user explicitly activates the desired service, and specifies what kind of local information she is interested in. The user is presented with information telling her what kinds of data (e.g., local position and/or identity) are transferred and to whom it is transferred. For convenience reasons the user can configure her privacy settings to specify that some information is transferred automatically under certain conditions.

One specific risk in the Finding Location and Guiding scenario is that the user may be provided by erroneous or suboptimal locations biased by for example commercial factors. Therefore the PRIME architecture should provide means for dispute resolution. For example, user should be supported in cases where she has been provided with erroneous or suboptimal information biased by commercial relationships between the LBS provider and other service partners;

Multi-user (P2P) scenarios (Person Finder, Mobile Dating): For multi-user scenarios, so called *reachability functionalities* [113] should be implemented. Reachability functionalities make it possible for users not only to specify which other users can localise them, but also *under which conditions* they are willing to be localised. For example, when Alice wants to localise Bob, she can provide additional information to Bob specifying the reason for the localisation. This information could include the urgency level and the subject for the localisation. For example, Alice could request for an urgent localisation in order to initiate a spontaneous meeting. Further,

the users should be able to specify whether they accept to be localised by a user not in their friend/dating list.

Additionally, it should be possible to specify the accuracy of the localisation. For example, a user could specify in her privacy policies that her friends only can receive the location with an accuracy of 10 km. Furthermore, only other end users should have the possibility to connect a user's current location to her real identity. In a PRIME-based solution LBS providers do not link users' locations to their real identities; instead schemes based on pseudonyms are used.

Any personal data stored in profiles and preferences can only be accessed when they were classified for publication to other users of the service. For example in the Mobile Dating scenario, unless the users choose to use a journal of their dates, no history of user interactions should be stored on the dating system;

Mobile Commerce scenario: In a PRIME-based solution, a mobile commerce application acts as a trusted intermediary which ensures that no identifying information about the users is passed on to the advertisers. Advertisers only receive information about profile matches. In return, neither the LBS provider nor the intermediary can collect information about the user's shopping behaviour without the user's explicit consent. This application is not allowed to sell profiles with identifying information to other parties. The users must be able to configure with a fine granularity the conditions under which they allow what kind of commerce information to be pushed to them; in particular, they have to be able to turn off offenders and limit the amount of information received;

Disaster Manager scenario: A PRIME supported disaster management infrastructure with mobile phone networks manages subscriber identities. By means of anonymization, pseudonymisation and data minimisation and based on stringent access control and authentication, only the information necessary is revealed at any given time. The disaster status of a region triggers permissions to be granted in a particular situation. In general, when users register other persons or locations for disaster information, no location or person shall be observed without consent. LBS providers should provide pseudonymisation technologies on the interfaces to the disaster management system, even though in some emergency situations, it is in the interest of the user that the disaster manager knows her identity, e.g. for finding and notifying her relatives. Information about the users' identity should not be available to anyone on the disaster management system unless there is strong evidence for a crime or a very critical individual situation, for example when there is a risk for loss of human life or destruction of valuable property.

In Table 5 below a summary of the application specific privacy requirements for the different LBS scenarios follows.

Table 5 – Application specific privacy requirements.

Requirement	Textual description	Application
Dispute resolution	The user should be provided with means to handle situations where she has been provided by erroneous or suboptimal guiding instructions	Finding Location
Specify accuracy of localisation	The user must be able to control the accuracy of the localisation	Mobile Dating, Person Finder
Allow/disallow "anonymous" localisation	The users of a PRIME-based person finder can specify whether they accept to be localised by a user not in their friend/dating partner list	Mobile Dating, Person Finder
Specify rules on a "per-friend" basis	Possibility to specify privacy preferences on a "per-friend" basis. In-depth control over what information are released to which friends/dating partner	Mobile Dating, Person Finder
Reachability functionalities	Reachability functionalities[49] allowing the users to specify under which circumstances they are willing to be localised on a "per friend" basis	Mobile Dating, Person Finder
Anonymous reputation building	Despite user anonymity, a reliable reputation building scheme should be implementable	Mobile Dating, Person Finder
Accuracy reduction filters	Some mechanism should exist that reduces the data accuracy (e.g. localisation precision)	Mobile Dating, Person Finder
Profile management	Any personal data stored in profiles and preferences can only be accessed when they were classified for publication to other users of the service	Mobile Dating, Person Finder
Control over commerce information	Users must be able to configure conditions under which what kind of commerce information may be pushed to them with fine granularity	Mobile Commerce
User control and consent	The users must have the possibility to configure who is allowed to receive disaster warnings in their whereabouts; property owners must consent in alerts generated about their property	Disaster Manager
Use of pseudonyms	Information about the users' identity shall not be available to anyone on the disaster management system unless there is strong evidence for a crime or a very critical individual situation	Disaster Manager
Restricted access to general observation mode	The "general observation mode" shall only be available after a disaster has been declared	Disaster Manager
Transparency for the users regarding available collection policies	Clear policies of use and guidance for users (e.g. with respect to lawful interception or the exact circumstances of disaster situations) shall be documented	Disaster Manager

[49] In the context of telephone communications, *reachability management* [7] means that the callees (receivers of a phone call) have the possibility to specify the circumstances under which they are willing to receive a call. Then, when a caller calls a callee, she attaches extra information explaining the reasons for making the call (e.g. urgency level or subject of the phone call). This information is compared to the preferences of the callee to make a decision whether the call should be accepted or not.

6.2.5 Role of Intermediaries in LBS

The telecommunication business is strongly dependent on re-sellers of their services. Classic business like directory service, fixed-line-leasing, number management, SMS clearing and mobile contract selling are usually provided by 3rd parties which are contracted by the mobile operator. For the upcoming market for location data, a large-scale business model will be constructed following this proven business model of the telecommunications industry.

Depending on what party does the localisation and the service provisioning, LBS business models can be distinguished into the following scenarios:

Direct localisation scenario: Mobile devices and application providers take care of localisation and application processing. The mobile network is used as a data channel;

Operator-portal scenario: Mobile operator offers the localisation and application. Here, we do not find any external application provider, because this is part of the operator's portal;

Application provider scenario: Mobile operators deliver communication and localisation, but the LBS are provided by independent application providers;

Intermediary scenario: Intermediaries collect localisation information from various sources (operators, GPS, WLAN), aggregate it and serve as a location broker for application providers.

The economic advantages of upcoming intermediary scenarios are:

Interoperability: An intermediary provides an interface for LBS providers, allowing them to access location data in a unified way;

Multi-channel strategy: An intermediary can collect location data from various sources (GSM, WLAN, and GPS);

Synergetic location aggregation: An intermediary can aggregate multi-channel location information for the benefit of higher quality (see [92] see for an algorithm);

Simplification: An intermediary simplifies process handling for LBS providers by removing the need to negotiate contracts with various location sources;

Cross-Operator applications: Without an intermediary, the creation of user-to-user LBS with customers using mobile services at distinct mobile operators is much harder;

Pricing advantages: Intermediaries provide many economic benefits in information markets, e.g. an intermediary buys location information from location providers in large amounts, and therefore is in a position to negotiate cheaper prices. Intermediary location data might be cheaper to acquire from an intermediary than from a location provider for LBS that consume small amounts of location data. Other benefits of information intermediaries can be found in [119][119].

Thus, the PRIME LBS design considers the intermediary scenario thoroughly to enable PRIME technology to be used in and applied for large-scale LBS business.

An Intermediary provides a platform that should make the provisioning of new location based services more feasible. The necessary functionality supported by the intermediary can be divided into consent management, location management and identity management. Note that the overall paradigm of the user managing her personal data is extended (instead of undermined or abandoned).

Consent management deals with the requirement that a user has to give her explicit consent before using a LBS application. An intermediary based distributed infrastructure needs to assure that the policies at the mobile operator and the LBS provider are consistent. These policies constrain under which conditions the user may be localised. If the mobile operator has proof of the users consent, location data is released to the intermediary.

Now the intermediary can do location management. The intermediary may store user-specific areas of interest entered by the LBS provider or the user herself. The intermediary then evaluates a push condition - e.g. the user being within an area with allergens. As the intermediary does not know the

user by name and does location management for a multitude of services, the intermediary should not be able to infer personal information.

In identity management systems pseudonyms are the core mechanism of privacy aware identity management. Each pseudonym and the data linked to it comprise an on-line identity, or partial identity, of the user. The unlinkability of these partial identities at the mobile operator, the intermediary and the LBS provider is an important privacy protecting feature of an intermediary architecture.

6.2.6 Outline of a PRIME-based architecture solution

The LBS scenarios require mechanisms in addition to the currently defined PRIME architecture. For the LBS scenarios, the following players can be identified: the *user (U)*, the *LBS provider(A)*, the *location intermediary (I)* and the *mobile operator (M)* as outlined further above in the scenario description. Each of the parties runs an IDM system and appropriate applications as specified in chapter 5 on the PRIME architecture.

6.2.6.1 Registration

In case the user wants to consume a location based service she first has to establish secure anonymous channels from the user to the LBS provider, between the LBS provider and the location intermediary and between the location intermediary and the mobile operator. For the channels between the LBS provider and the location intermediary and the location intermediary and the mobile operator both endpoints of the channels are untrusted and it must not be possible for either of the connected parties to infer the identity (or address) of the respective other party via the channel. The channels are established with the support of the user. The channels are exclusively used for data communication regarding data of this single user. Each party receives a pseudonym to be associated with the channel. At the location intermediary, the pseudonym links together the two channels to the LBS provider and to the mobile operator being used for providing a location based service to the user. For example, the pseudonym n_IU (see Figure 21) links the channel between the LBS provider and the location intermediary with the channel between the location intermediary and the mobile operator. See Figure 21 for the typical setting in location based services. The lines with arrows represent channels, the labels of a channel sketch what is being performed over the channel.

After the channels have been established the user starts a trust negotiation process with the LBS provider to provide the personal data required for the service provision and to make the required payment. It is important to note that the data being disclosed shall not identify the user. Next, a trust negotiation process is executed with the location intermediary. Then, a trust negotiation process is executed with the mobile operator. In each trust negotiation instance the privacy compliance of the party is assessed, a data handling policy for the disclosed data including location data is negotiated, and the party is authenticated. Depending on the granularity on which user consent is required, consent for the data processing is given. As a last step, the service provision is triggered by the user. The approach outlined above is common to a large class of location based services, so called push services. In the following paragraph we consider a “push scenario” such as a pollen warning scenario where the user is warned in case she enters a region contaminated with pollen she is allergic against.

6.2.6.2 Operation

The user discloses to the LBS provider information on which pollen she is allergic against. The LBS provider obtains the distribution of important kinds of pollen from third parties in regular time intervals. The LBS provider sets the regions at the location intermediary which contain pollen set by the user. The LBS provider requests an alarm from the location intermediary when the user enters one of the regions. The location intermediary requests locations from the mobile operator in regular time intervals and performs a matching of the location with the defined regions. In case of a match, the LBS provider is informed of the match and the zone. The LBS provider then informs the user of the pollen in her current location over the anonymous channel.

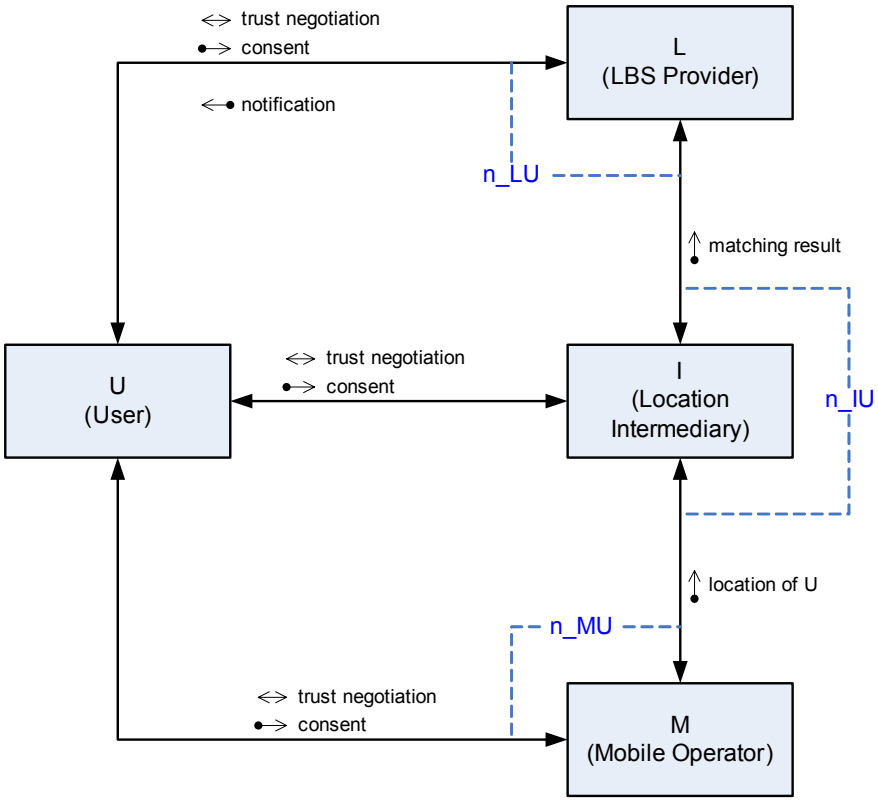

Figure 21 Infrastructural setting for location based services

6.2.6.3 Privacy Protection

The set-up outlined above provides very high protection of the user's privacy.. The data provided by the user shall not allow identifying the user. The location intermediary does not obtain application-specific information such as the pollen the user is allergic against, but gets only regions to match against without any semantics attached to the regions. The location intermediary receives only coordinates of the user from the mobile operator without knowing the identity of the user. The mobile operator knows the location and identity of the user and can track the user. This seems to be unavoidable considering the current mobile communication infrastructures. Only anonymous prepaid schemes solve this problem partly but cannot be considered the main target group[50]. Due to the properties of the anonymous channels it is feasible that the location intermediary does not get to know the mobile operator or the LBS provider nor that the LBS provider gets to know the mobile operator. Also, the information revealed to the location intermediary may be obfuscated, hiding e.g. specific allergies from the intermediary service. Thus it is infeasible for the parties to pool the information they have obtained about the user. Consent that has been given can be revoked by collapsing the channels which is possible since the user retains control over the channels during the lifetime of the channels. This revocation of consent is fully enforceable by the user and thus does not rely on the other parties for its enforcement.

6.2.7 A First Approach

In order to evaluate the possibilities of building a PRIME based LBS solutions as outlined in 6.2.6 a prototype has been developed. The prototype follows in essence the infrastructural setting described in Figure 21 whit the exception that the notification is initiated by LBS Provider, but not transmitted directly. The prototype has been developed by T-Mobile in cooperation with University of Frankfurt. For T-Mobile, the prototype leads to new insights into how privacy enhanced identity management can be introduced into an m-commerce scenario without restricting the business models. An idea on how

[50] Note that anonymous pre-paid schemes could still be linkable (via e.g. movement profiles), leading to possible identification by the mobile operator anyway

privacy enhancing services can be deployed within a telecommunication environment, especially as a standardized identity management system, can enable new and efficient business models in such a scenario. Also, T-Mobile decided to develop a product based on the prototype For a more in-depth discussion on the prototype and commercialisation plans see the description in the forthcoming PRIME Book.

7 The Landscape of Identity Management

7.1 Current Identity Management Areas and Solutions

Today, many identity management products and solutions are available on the market. They supply functionalities such as authentication, SSO, authorization, auditing, provisioning, data storage, links to legacy systems and data consolidation. They target different types of users and contexts including eCommerce, service providers, enterprises and government institutions.
Figure 4 shows the main components and functionalities provided by current identity management products and solutions:

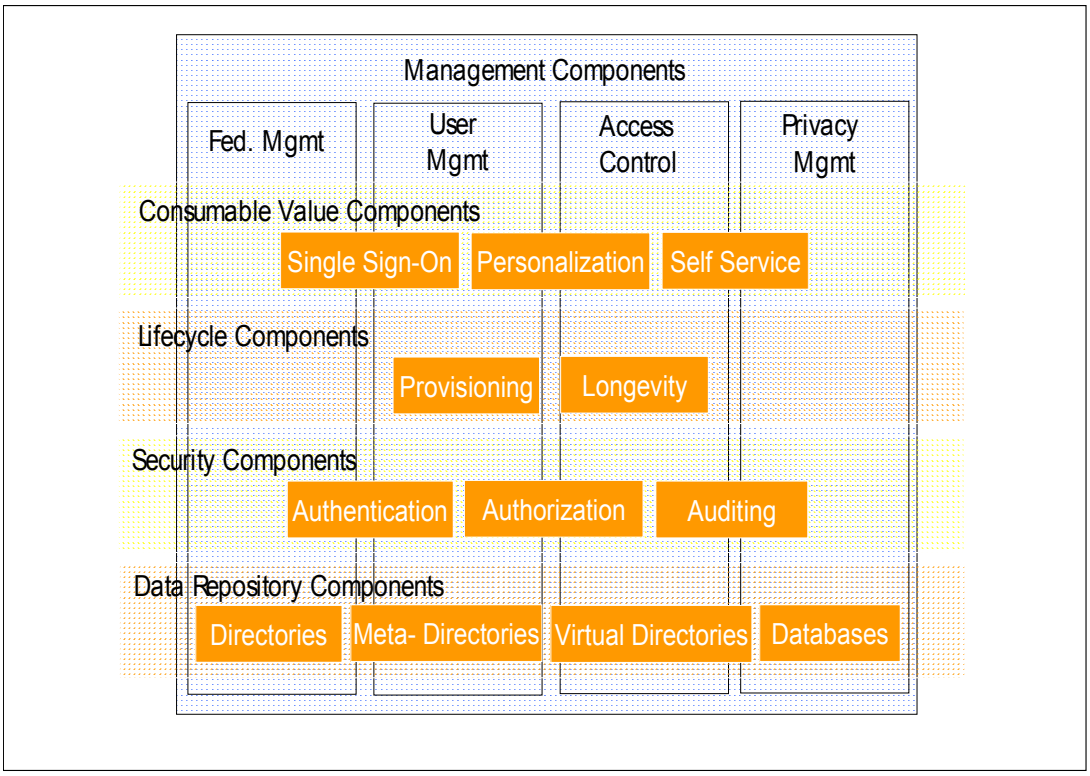

Figure 22 Current Identity Management Solution Stack

Directory services and meta-directories deal with the representation, storage and management of identity and profiling information and provide standard APIs and protocols for their access. In particular, meta-directories address the important problem (especially for large organizations and enterprises) of consolidating, integrating and preserving the consistency of data, disseminated in a variety of heterogeneous systems, geographically spread across organization sites.

Authentication, authorisation and auditing are core identity management functionalities. Authentication, in particular, is provided in a variety of ways ranging from local authentication on a system to complex distributed authentication, including single-sign-on (SSO) within and across organizational boundaries. Recent initiatives, including Liberty Alliance Project, aim at the provision of SSO for a federated environment, by leveraging identity providers acting as trusted third parties. Similarly, authorization functionalities are provided in a variety of forms, usually coupled with auditing capabilities. Authorization can include simple access control management at the OS level, more sophisticated role-based access control - RBAC [94] - up to flexible, distributed, policy-driven authorization, at the application and service levels.

Provisioning and accounting solutions are used by enterprises, organizations and eCommerce sites to deal with the enrolment, customization, modification and destruction of accounts associated to users,

employees and customers along with associated identity information (including rights, permissions and access control information).

Life-cycle management solutions deal with the issuance, certification, management and revocation of digital entitlements and credentials in a secure and trusted way. In particular PKI-based solutions are available for this purpose but their adoption is not so widespread, especially in inter-organizational contexts, because of the intrinsic trust management problems, the complexity of CA hierarchies and related costs.

Web-services and the forthcoming web-services standards are also having an impact on identity management, especially for aspects concerning the management of identities for web services, single-sign on and federated identity management.

The above components and solutions have been described from an enterprise and organizational perspective: this is where identity management solution providers are concentrating most of their efforts and where, currently, most of the money is.

In the context of enterprise identity management, privacy requirements are currently marginally addressed by means of technological solutions, specifically in terms of controlling accesses to PII data, according to well defined policies and preferences.

Quite often enterprise privacy management consists of "manually" applying good practices, policies and human processes or relying purely on current security solutions. This is expensive and prone to mistakes.

The PRIME project has contributed to improve the current situation in this space by introducing technology and automation (PRIME Toolbox), in terms of ways to control accesses of personal data and enforce security and privacy policies by keeping into account data handling criteria, data purposes and users' consent. See Section 5.4 for more details on what PRIME provides.

Many new initiatives are also emerging in the context of "federated identity management" which involves a wider set of stakeholders, including users, service providers and identity providers. In this context, privacy is a primary concern. Next section provides a more detailed overview of some of the current initiatives.

7.2 Federated Identity Management Initiatives

Various initiatives are emerging in the Federated Identity Management Landscape, including the following ones (see section7.5 for more technical details) :

- Liberty Alliance ID-FF;
- OpenID;
- WS-Federation;
- Microsoft CardSpace;
- Higgins;
- Novell's Bandit;
- Shibboleth.

From a technology point of view, we can distinguish, from a trust model perspective, between two quite different types of systems: 1) Traditional token-based identity management and 2) anonymous-credential-based identity management.

7.2.1 Traditional Token-based Systems

The *traditional token-based systems* are based on an Identity Provider (IdP) who mediates each transaction and creates a federation token or message that is provided to the Relying Party (RP) where the RP is the service provider the user wants to give identity attributes to. The major drawbacks with those systems are that the IdP learns about each transaction the user does and what information is used

in each transaction. That is, the IdP can profile the user. An advantage of such systems is that revocation is trivially achieved by the IdP not issuing further tokens once (parts of) an identity have been revoked.

Within this class of systems, we can distinguish between systems that feature two types of systems based on whether the user is required to install software: *Zero-footprint solutions* are ones where there is no need for installing software on the user side, but they are purely browser based. *Active client solutions*, on the other hand, require the user to have software installed or shipped with their system.

Zero-footprint browser-based solutions are characterized as follows:

- Easy to deploy as no software installation is required
- Fewer adoption barriers
- No need for users to manage tokens locally

Active-client solutions have the following key properties:

- Better for user privacy as the active client can help in giving less information to the IdP
- The user needs to take care herself for securing their credentials and providing for backup
- Harder to deploy due to the software installation requirement

7.2.2 Anonymous Credential-based Systems

Systems based on *anonymous credentials* allow that users obtain anonymous credentials that have longer life-time and can be used by the user to endorse identity attributes at RPs without involving the IdP. As a particular advantage, the Identity Provider does not have the ability to profile the user. Anonymous credential systems allow for anonymous and unlinkable transactions unless identifying information is needed in the transaction. That is, credential systems allow users to provide certified attributes to service providers while fully controlling the transaction and not involving the IdP in the transaction.

Two prominent examples of anonymous credential systems are the systems of Brands [11] and Camenisch and Lysyanskaya [11]. The latter is also known as *identity mixer* or *idemix* in short. Anonymous credential systems are always active-client solutions due to the inherent requirement of performing computations on the client in order to obtain the desired features. As of today, there are no deployments of anonymous credential systems yet, but substantial interest has come up in the identity management community in pushing this technology towards deployment. An example for this is the Higgins project that is, among more traditional technologies, also looking at anonymous credential systems.

7.3 How PRIME Relates to Other Initiatives

PRIME is mainly targeting the privacy aspect of the user-related parts of the identity management stack. Though, PRIME is not limited to the “front-end”, or user-facing, part of identity management, but its approach to privacy policies also helps in the “back-end” part in terms of enforcing usage control.

More precisely, PRIME’s focus is on making data minimising transactions between users and service providers or other users possible while still maintaining the security of attributes in terms of endorsement of attributes by identity providers. PRIME uses anonymous credential systems as its core identity federation technology and thus gives more control to the user on releasing their data than any other technology. Transactions are done such that identity providers learn the least possible amount of information, thus their ability to profile the users is limited.

Elaborating further on the user-side aspects on which PRIME improves on the state of the art raises the issue of user consent, privacy policies, trust, and user interfaces. The main idea is that the user gets the same user interface regardless of the service provider or identity provider she is interacting with. This helps improve on security as the user only needs to learn one particular interface and not one for each organization she interacts with. Microsoft CardSpace, the Higgins open source initiative, and Novell’s

Bandit take the same approach of having an active client solution with an easy-to-use interface. Though, PRIME was the first of those pursuing this idea and has a broader coverage and more progressive approach in terms of privacy protection. None of the other approaches currently includes an approach to data handling policies using a formal policy language and not the usual free-form privacy statement. Another distinguishing feature of PRIME is the possibility of an assessment of a service provider regarding its trustworthiness. This allows a user to judge whether it is safe to share (personal) data with a particular service provider.

From a server-side perspective, PRIME comes with an advanced solution for access control that allows for attribute-based access control and thus more dynamic system behaviour than systems that do not integrate with an access control solution in such a tight manner. Considering the management of identities at the server side, PRIME features a life-cycle data management solution that can enforce policies like limited-time data retention or user notification on the policy enforcement. PRIME features a sticky-policy approach of keeping data associated to their data handling policy from the creation to the data until their (policy-defined) destruction. Clearly, this requires that every party involved needs to have PRIME technology deployed in order for leveraging the full data protection of PRIME. It is clearly a challenge and will take time to get such a technology stack deployed and widely-adopted in practice.

Overall, PRIME, as a research project, takes a more comprehensive approach towards privacy in identity management than industry initiatives as those typically take a more pragmatic approach towards identity management and have a lesser focus on comprehensive protection of user privacy. Considering the above discussion, PRIME has various technologies that will be interesting for other initiatives to have a look for future adoption.

7.4 Deployment

Traditional systems are available those days, commercial products and open source products are available. Microsoft has deployed already their CardSpace system that is based on WS-Federation as underlying protocol suite. It is deployed with every installation of their new operating system.

Particularly URI-based systems are in a hype currently, probably due to their simplicity. Security is not sufficient, though.

Anonymous credential systems are not deployed in real-world systems those days, they are used in research, though. Currently, multiple industry and open source players show interest in this technology due to the privacy and user control advantages the technology brings to the users.

In general, their main focus has been to provide single-sing-on frameworks, for distributed scenarios where users can interacts with multiple service providers, potentially mediated by one or more identity providers.

Ultimately personal information is used and exchanged between stakeholders, to enable users' interactions. Different kind of approaches are using, ranging from simple disclosures of personal data via self-service registration portals, to more sophisticated certified credentials and/or assertion tokens (e.g. MS InfoCard, SAML tokens, etc.).

Trust and privacy aspects are key issues for all these frameworks, due to the distributed nature of federated identity management and the need to potentially disclose personal information to multiple parties.

Privacy management initiatives are currently in their early stages, for example in the context of Liberty Alliance, MS CardSpace and OpenID. More has to be done to fully take into account fine-grained user preferences, manage users' expectations and automatically handle and enforce privacy policies and guidelines at the service side.

7.5 Overview: Identity Management Initiatives

The remaining part of this chapter provides more technical details about these various initiatives in the identity management framework. Descriptions of these initiatives have been retrieved from related web sites and Wikipedia.

7.5.1 Liberty Alliance

The Liberty Alliance was formed in 2001 by approximately 30 organizations to establish open standards, guidelines and best practices for federated identity management. Liberty Federation (ID-FF), released in 2002, allows consumers and users of Internet-based services and eCommerce applications to authenticate and sign-on to a network or domain once from any device and then visit or take part in services from multiple Web sites. This federated approach does not require the user to reauthenticate and can support privacy controls established by the user. The market requirements documents and case studies of deploying organizations, as well as presentations of deployments are available. The Liberty Alliance contributed its federation specifications, ID-FF, to OASIS, forming the foundation for SAML 2.0, the converged federation specification that Liberty now recognizes.http://en.wikipedia.org/wiki/Image:Liberty-actors.jpg Recent Liberty Alliance initiatives of relevance to privacy include:

- Liberty Alliance Identity Governance Framework (IGF)
- Liberty Alliance Identity Capable Platforms (ICP) in the context of the LA Advanced Client Technologies initiative
- Liberty Alliance Identity Assurance

7.5.2 OpenID

OpenID is a decentralized single sign-on system. Using OpenID-enabled sites, web users do not need to remember traditional authentication tokens such as username and password. Instead, they only need to be previously registered on a website with an OpenID "identity provider". Since OpenID is decentralized, any website can employ OpenID software as a way for users to sign in; OpenID solves the problem without relying on any centralized website to confirm digital identity.

7.5.3 WS-Federation

WS-Federation is an Identity Federation specification part of the larger Web Services Security framework, WS-Federation defines mechanisms for allowing disparate security realms to broker information on identities, identity attributes and authentication. WS-Federation extends WS-Trust to provide a flexible Federated Identity architecture with clean separation between trust mechanisms, security token formats, and the protocol for obtaining tokens. This architecture enables a reusable security token service model and protocol to address the identity requirements of both web applications and web services in a variety of trust relationships. The features of WS-Federation can be used directly by SOAP clients and web services. WS-Federation also defines syntax for expressing the WS-Trust protocol and WS-Federation extensions in a browser based environment. The intention of this functionality is to provide a common model for performing Federated Identity operations for both web services and browser-based applications.

7.5.4 MS CardSpace/InfoCard

Windows CardSpace (codenamed InfoCard), is Microsoft's client software for the Identity Metasystem. CardSpace is an instance of a class of identity client software called an Identity Selector. CardSpace stores references to users' digital identities for them, presenting them to users as visual Information Cards. CardSpace provides a consistent UI that enables people to easily use these identities in applications and web sites where they are accepted. When an Information Card-enabled application or website wishes to obtain information about the user, the application or website requests a particular set of claims from the user. The CardSpace UI then appears, switching the display to the CardSpace service, which displays the user's stored identities as visual Information Cards. The user selects the InfoCard to use and the CardSpace software contacts the issuer of the identity to obtain a digitally signed XML token that contains the requested information. CardSpace allows users to create personal (also known as self-issued) Information Cards. Other transactions may require a managed InfoCard; these are issued by a third party *identity provider* that makes the claims on the person's behalf, such as a bank, employer, or a government agency.

7.5.5 Higgins

Higgins is an open source framework that enables users and other systems to integrate identity, profile, and relationship information across multiple heterogeneous systems. Higgins unifies all identity interactions (regardless of protocol/format) under a common user interface metaphor called i-cards. Higgins enables developers to write to a common API for Identity management, rather than needing to support multiple identity management systems individually. Software applications written to Higgins will allow people to store their digital identities and profile information in places of their choice and to share the stored information with companies and other parties in a controlled fashion.

7.5.6 Bandit Project

The Bandit project is an open source collection of loosely-coupled components to provide consistent identity services. It implements open standard protocols and specifications such that identity services can be constructed, accessed, and integrated from multiple identity sources. Portions of the identity services are an implementation of the Higgins trust framework. The Bandit system supports many authentication methods and provides user-centric credential management. On this base of a common identity model, Bandit is building additional services needed for Role Based Access Control RBAC and for the emission of records to verify compliance with higher level policies.

7.5.7 Shibboleth

Shibboleth is an Internet2 Middleware Initiative project that has created an architecture and open-source implementation for federated identity-based authentication and authorization infrastructure based on SAML. Federated identity allows for information about users in one security domain to be provided to other organizations in a common federation. This allows for cross-domain single sign-on and removes the need for content providers to maintain usernames and passwords. Identity providers supply user information, while service providers (SPs) consume this information and gate access to secure content.

8 Conclusions

The PRIME Framework V3 presented in this document follows an interdisciplinary approach and discusses emerging privacy problems, defines the vision of the project and provides the PRIME requirements and a holistic solution for privacy-enhancing identity management. The presented PRIME solution is not only technically feasible, but also based on the European regulatory and legal framework, and furthermore also aims to be socially acceptable and desirable, economically exploitable, intuitive and user-friendly, and deployable by applications.

In particular, PRIME Framework V3 starts by defining key terms and definitions, and then elaborates the problem space by describing trends in personal data use from a technological, legal, business to a societal perspective, by describing the consequences of increased personal data use for the individual and society, and by showing where current solutions fall short and where PRIME could help. It provides and integrated view on the legal, social economic requirements to be addressed to reach to a PRIME solution. It then presents the PRIME solution for realising the PRIME vision of restoring the control of users over their personal spheres and in particular shows how the PRIME solution addresses the PRIME design principles as the core of PRIME's vision. For this, it introduces a privacy management framework as part of the PRIME solution, which is embedded in the life cycle of services and discusses the development of core processes and the social, legal, economic impacts on these in the various phases of the life cycle, and links them with the PRIME architecture. It also describes the user side processes and identity management tasks, links these to the PRIME architecture, and discusses UI design proposals supporting user side processes. Finally, the PRIME eShopping and LBS application scenarios illustrate how PRIME can be integrated into privacy-sensitive applications.

Besides, the PRIME Framework demonstrates that the PRIME solution can enhance privacy for the end users by allowing service providers to conduct their legitimate business interests and activates with less or no personal data processing. The PRIME solution applied by businesses can thus in turn increase customers' trust in businesses and become a business enabler.

9 References

[1] Ahn, T., Ryu, S., & Han, I. . *The impact of the online and offline features on the user acceptance of internet shopping malls*. Electronic Commerce Research and Applications, 3, pp. 405-420, 2004

[2] *American Library Association E-Government Act of 2002- Details and Background*, American Library Association (ALA), http://lita.org/ala/washoff/woissues/governmentinfo/egovernment/backgroundab/background.cfm.

[3] Andersson, C., Camenisch, J., Crane, S., Fischer-Hübner, S., Leenes, R. E., Pearson, S., Pettersson, J. S., & Sommer, D. *Trust in PRIME*. In Proceedings of the 5th IEEE Int. Symposium on Signal Processing and IT 2005, Athens, Greece ,December 18-21, 2005.

[4] Article 29 Data Protection Working Party. *Opinion on More Harmonised Information Provisions*. Tech. rep., EU, 2004.

[5] Article 29 Data Protection Working Party. *Opinion 5/2005 on the use of location data with a view to providing value-added services*. Tech. rep., EU, 2005.

[6] Blanchette, J.-F., & Johnson, D. G. *Data retention and the panoptic society: The social benefits of forgetfulness*. The Information Society, 18, pp. 33-45, 2002.

[7] Bangerter, E., Camenisch, J., & Lysyanskaya, A. *A cryptographic framework for the controlled release of certified data.* In Twelfth International Workshop on Security Protocols 2004 , LNCS, Springer Verlag, 2004.

[8] Bergmann, M., Rost, M., & Pettersson, J. S. *Exploring the feasibility of a spatial user interface paradigm for privacy enhancing technology.* In: Proceedings of the Fourteenth International Conference on Information Systems Development (ISD2005) Springer Verlag, 2005,.

[9] Bergmann, M. *Generic Predefined Privacy Preferences for Online Applications*. In: Proceedings of the 3rd IFIP/FIDIS Summer Schon on "The Future of Identity in the Information Society", Karlstad, 4-10 August 2007, to appear at Springer Verlag, 2008.

[10] PRIME Consortium.. Requirements v3 (forthcoming) (Deliverable): PRIME Consortium, 2008.

[11] Brands, S. A. *Rethinking public key infrastructures and digital certificates*, MIT Press, 2000.

[12] Camenisch, J., & Lysyanskaya, A. *Efficient non-transferable anonymous multi-show credential system with optional anonymity revocation.* In Advances in Cryptology — EUROCRYPT2001, Pfitzmann, B. Ed., vol. 2045 of LNCS, Springer Verlag, pp. 93–118, 2001.

[13] Cameron, K. *The laws of identity*: Microsoft Corporation, 2005.

[14] Cantor, S., & Kemp, J. *Liberty ID-FF protocols and schema specification*, 2003.

[15] Carey, P. *E-Privacy and Online Data Protection*, Butterworths, pp.58, 2002.

[16] CEN. *Personal Data Protection Audit Framework (EU Directive 95/46) Part I: Baseline Framework*. Tech. rep., CEN, February 2006.

[17] Chan, H., & Perrig, A. *Security and Privacy in Sensor Networks*. Computer, October, 2003.

[18] Chaum, D. *Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms.* Communications of the ACM 24, 2, pp. 84-88, 1981.

[19] Chaum, *D. Security without Identification: Transaction Systems to Make Big Brother Obsolete.* Communications of the ACM 28, 10, pp. 1030-1044, 1985. http://www.chaum.com/articles/Security_Wthout_Identification.htm.

[20] Clarke, R. A. *Information Technology and Dataveillance*. Communications of the ACM, May, 1988.

[21] Clauss, S. & Köhntopp, M. *Identity management and its support of multilateral security.* Computer Networks, 37, pp. 205-219, 2001.

[22] Collins, C. *English dictionary for advanced learners*, 2001.

[23] Commission European Communities. *I2010 – Annual information society report 2007 (No. COM(2007) 146 final)*. Brussels, 2007.

[24] *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Radio Frequency Identification (RFID) in Europe: steps towards a policy framework*, COM(2007) 96, 2007.

[25] Courtney, P., Lacey, C., & Nash, R. *Privacy in the digital networked economy*. London: HenleyCentre, 2005.

[26] Council of Europe. *European Convention of Human Rights (ECHR).* Rome, 4 November 1950.

[27] Council of the European Union, Statements, *Council doc. 5777/06 ADD 1*. February 10, 2006 available at http://register.consilium.eu.int/pdf/en/06/st05/st05777-ad01.en06.pdf.

[28] Council of the European Union. *Agreement between the EU and the USA on the processing and transfer of PNR data by air carriers to the United States Department of Homeland Security*. Brussels, 2007.

[29] Courtney, P., Lacey, C., & Nash, R. *Privacy in the digital networked economy*. London: Henley Centre, 2005.

[30] Culnan, M. J., & Armstrong, P. K.. *Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation.* Organization Science, 10(1), pp. 104-115, 1999.

[31] De Noord, D., & Attema, J. *Second life; het tweede leven van virtual reality.* The Hague: EPN, 2006.

[32] Deming, E. *Out of the Crisis*. Center for Advanced Engineering Study, MIT, 1986.

[33] DiMaggio, P., & Hargittai, E. *From the 'digital divide' to 'digital inequality': Studying internet use as penetration increases*: Center for Arts and Cultural Policy Studies, Woodrow Wilson School of Public and International Affairs. Princeton University, pp. 19, 2001.

[34] Directorate-General Information Society and Media. *Broadband access in the EU: Situation at 1 July 2007 (No. COCOM07-50 FINAL).* Brussels: European Commission, 2007.

[35] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, O.J. L 281, 23.11.1995

[36] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, O.J. L201, 31.07.2002, pp. 37 – 47.

[37] Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, Official Journal L105, 15 March 2006, pp. 54.

[38] Donath, J., & Boyd, D. *Public displays of connection.* BT Technology Journal, 22(4), pp. 71-82, 2004.

[39] Donath, J. S. *Identity and deception in the virtual community.* In P. Kollock & M. Smith (Eds.), Communities in cyberspace. London: Routledge, 1998.

[40] EPIC, & Privacy International. *Privacy & human rights*. Washington, 2006.

[41] European Data Protection Supervisor, *First opinion on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters (COM (2005) 475 final)*, OJ C 47, 25. February 2006, par. 10.

[42] European Data Protection Supervisor, *Opinion on the Initiative of the Federal Republic of Germany, with a view to adopting a Council Decision on the implementation of Decision 2007*/…/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, 19 December 2007

[43] European Digital Rights,. *Electronic voting machines eliminated in the Netherlands*. EDRI-gram, 5, 24 October 2007. http://www.edri.org/.

[44] Fano, A., & Gershman, A. *The future of business services in the age of ubiquitous computing.* Communications of the ACM, 45(2), pp. 83-87, 2002.

[45] Ferer, M. *Media Player and Privacy.* Seattle Weekly, 1999.

[46] Figge, S., Schrott G. *3G "ad" Work - 3G'S Breakthrough with mobile Advertising*. In: Proceedings of the 8th International Workshop on Mobile Multimedia Communications; Munich, 2003.

[47] Fichman R.G. *Information Technology Diffusion: A Review of Empirical Research*. Proceedings of the Thirteenth International Conference on Information Systems (ICIS), Dallas,, pp. 195-206, 1992.

[48] Fleischer, P. *The need for global privacy standards, Ethics and human rights in information society*. Strasbourg, 2007.

[49] Friedman, B., Kahn JR., P., & Howe, D. C. *Trust online*. Communications of the ACM, 43(12), 34-40, 2000.

[50] Fritsch, L., Rannenberg, K. *Informationstechnische Voraussetzungen von E-Government am Beispiel des Katastrophenschutzes mittels Mobilkommunikation*. In: Tagungsband zur Jahrstagung 2002 der Deutschen Gesellschaft für Recht und Informatik, Otto-Schmidt-Verlag; Köln, 2001.

[51] Fritsch, L. *Mind your step! How profiling location reveals your identity and how you prepare for it*. In FIDIS Doctoral Consortium, Post-Proceedings on Profiling, October, 2005.

[52] Foucault, M. *Discipline and punish: The birth of the prison.* Londen: Allen Lane; Lyon, D. (2001). Surveillance society; monitoring everyday life. Buckingham: Open University Press, 1977.

[53] Foundation for Information Policy Research, UK Information Commissioner study project: privacy and law enforcement, Paper n°4: *the legal framework, an analysis of the constitutional European approach to issues of data protection and law enforcement* , pp.59, February 2004.

[54] Gasson, M., Meints, M., & Warwick, K. (Eds.), *FIDIS Project Deliverable D3.2: A Study on PKI and Biometrics.* Tech. rep., FIDIS, July 2005.

[55] Gavison, R. *Privacy and the limits of law*. The Yale Law Journal, 89(3), pp. 421-471, 1980.

[56] Grance, T., Hash, H., & Stevens, M. *Security considerations in the information development life cycle.* NIST Special Publication 800-64 Rev. 1, National Institute of Standards and Technology, 2004.

[57] Greenhalgh T., et al., *Diffusion of innovations in service organizations: Systematic review en recommendations*. The Milbank Quarterly, 2004/4, pp. 581-629, 2004.

[58] Guenther, O., & Spiekermann, S. *RFID and the perception of control: The consumer's view.* Communications of the ACM Vol. 48, No. 9 (2005), pp.73–76, 2005.

[59] Heylighen, F. *Complexity and information overload in society: Why increasing efficiency leads to decreasing control*. The Information Society: Free University of Brussels, 2002.

[60] High Level Group. Facing *the challenge; the Lisbon strategy for growth and employment.* Luxembourg: European Communities, 2004.

[61] Hoffman, D. L., Novak, T. P., & Peralta, M. *Building consumer trust online: How merchants can win back lost consumer trust in the interest of e-commerce sales*. Communications of the ACM, 42(4), pp. 80-85, 1999.

[62] Hui, M. K., & Bateson, J. E. G. *Perceived control and the effects of crowding and consumer choice on the service experience.* Journal of Consumer Research, 18(2), pp. 174-184, 1991.

[63] Hustinx J. P. Intervention at the European Parliament (LIBE Committee) Public Seminar "Data Protection and citizens' Security: What Principles for the European Union?", Brussels, 31 January 2005, available online at http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2005/05-01-31_Seminar_LIBE_EN.pdf

[64] ICPP, and SNG. *Identity Management Systems: Identification and Comparison Study*. Tech. rep., Independent Centre for Privacy Protection (ICPP) and Studio Notarile Genghini (SNG), September 2003.

[65] Introna, L. D. *Privacy and the computer: Why we need privacy in the information society.* Metaphilosophy , 28(3), pp. 259-275, 1997.

[66] ISPTA. *Privacy Framework V1. 1.* International Security Trust and Privacy Alliance (ISPTA), 2002.

[67] Iyengar, S. S., & Lepper, M. R. *When choice is demotivating: Can one desire too much of a good thing?* Journal of Personality and Social Psychology, 79, pp. 995-1006, 2000.

[68] Jacobson, I. Booch, G. J.R. *The Unified Software Development Process.* Addison Wesley Longman, 1999.

[69] Johnson, D. G., & Miller, K. *Anonymity, pseudonymity, or inescapable identity on the net.* Computers and Society, 1998.

[70] Koops, B.-J., & Leenes, R. E. *Code and the slow erosion of privacy.* Mich. Telecomm. Tech. L. Rev. 12, pp. 115-188, 2005.

[71] Koops, B.-J. & Leenes, R. E. *Identity Theft, Identity Fraud and/or Identity-related Crime.* Datenschutz und Datensicherheit, pp. 553-556, 2006.

[72] Koops, B. J., Leenes, R., Meints, M., Van der Meulen, N., & Jacquet-Chiffelle, D.-O. *A typology of identity-related crime: Conceptual, technical, and legal issues*. (forthcoming): Tilburg Institute for Law, Technology, and Society, 2008.

[73] Kosta, E., Coudert, F. & Dumortier, J. *Data protection in the third pillar: in the aftermath of the ECJ decision on PNR data and the data retention directive*. International Review of Law, Computers and Technology, Volume 21, No. 3, pp. 343-358, November 2007

[74] Kroon R., van Gils H., ter Hart J., Overbeek P, Tellegen, P. Borking J., *Privacy Enhancing Technologies – Witboek voor beslissers*. Ministry of internal affairs and Kingdom relations; December, 2004.

[75] Kuner Ch., *European Data Protection Law – Corporate Compliance and Regulation,* Oxford University Press, 2007.

[76] Leenes, R. *Protecting privacy online: Law or technology?* (forthcoming): Tilburg Institute for Law, Technology, and Society, 2007.

[77] Lessig, L. *Code and other Laws of Cyberspace*. New York: Basic Books, 1999.

[78] Levi, M., & Wall, D. S. *Technologies, security, and privacy in the post-9/11 European information society.* Journal of Law and Society, 31(2), pp.194-220, 2004.

[79] Liberty Alliance Project. Whitepaper: *Personal identity*. March 23 2006.

[80] Lips, M., Taylor, J. A., & Bannister, F. *Public administration in the information society: Essays on risk and trust.* Information Polity, 10(1,2), pp.1-9, 2005.

[81] Lyon, D. *Surveillance society; monitoring everyday life*. Buckingham: Open University Press, 2001.

[82] Lyon, D. *Globalizing surveillance; Comparative and sociological perspectives.* International Sociology, 19(2), pp.135-149, 2004.

[83] Marbus, R. *Managing identities in online social environments.* (forthcoming): Tilburg Institute for Law, Technology, and Society, 2007.

[84] Marbus, R. *Personal identity in online environments* (forthcoming PhD thesis): Tilburg Institute for Law, Technology, and Society, 2007.

[85] Margulis, S. T. *Privacy as a social issue and behavioural concept.* Journal of Social Issues, 59(2), pp. 243-261, 2003.

[86] Martin, K., & Freeman, R. E. *Some problems with employee monitoring.* Journal of Business Ethics, 43, pp. 353-361, 2003.

[87] Marx, G. *Varieties of personal information as influences on attitudes toward surveillance.* In Conference on The New Politics of Surveillance and Visibility, 2003.

[88] McKenna, K. Y. A., & Bargh, J. A. *Plan 9 from cyberspace: The implications of the internet for personality and social psychology.* Personality and Social Psychology Review, 4(1), pp. 57-75, 2000.

[89] McKnight, D. H., & Chervany, N. L. *Trust and distrust definitions: One bite at a time.* In R. Falcone, M. Singh & Y.-H. Tan (Eds.), Trust in cyber-societies: Integrating the human and artificial perspectives (Vol. 2246/2001). Berlin: Springer Berlin / Heidelberg, 2001.

[90] Metzger, M. J. *Effects of site, vendor and consumer characteristics on web site trust and disclosure.* Communication Research, 33(3), pp. 155-179, 2006.

[91] Microsoft Corporation. *Microsoft's vision for an identity metasystem white paper*, May 2005.

[92] Myllymaki J. & Edlund S. *Location Aggregation from Multiple Sources*. Singapore: 2002.

[93] Nissenbaum, H. *Protecting privacy in an information age: The problem of privacy in public.* Law and Philosophy, 17, pp. 559-596, 1998.

[94] NIST (National Institute of Standards and Technology, Role-Based Access Control, http://csrc.nist.gov/groups/SNS/rbac/

[95] Olsen, T., Mahler, T., Seddon, C., Cooper, V., Williams, S., Valdes, M., et al. *Privacy & identity management*. Oslo: Senter for rettsinformatikk, 2007; Stalder, F. *The failure of privacy enhancing technologies (PETs) and the voiding of privacy.* Sociological Research Online, 7(2), 2002.

[96] Olivero, N., & Lunt, P. *Privacy versus willingness to disclose in e-commerce exchanges: The effect of risk awareness on the relative role of trust and control*. Journal of Economic Psychology, 25(2), pp. 243-262, 2004.

[97] O'Reilly, T. *What is web 2.0; Design patterns and business models for the next generation of software*. O'Reilly, 2005.

[98] Paniza Fullana, A. *DRM Sony system, consumer protection and user privacy*. In Proceedings of the First International Conference on Legal, Privacy and Security Issues in Information Technology, vol. Vol. 2, 2006, pp. 67–82, 2006.

[99] Petterson, J. S., Fischer-Hübner, S., Danielsson, N., Nilsson, J., Bergmann, M., Clauss, S. Kriegestein, Th., Krasemann, H., *Making PRIME Usable.* SOUPS 2005 Symposium on Usable Privacy and Security, Carnegie Mellon University Pittsburgh, PA, USA, July 6-8 2005 (also appeared in ACM Digital Library)..

[100] Pettersson, J.S., & Fischer-Hübner, S. *Transparency as the Key to User-controlled Processing of Personal Data*. In Human IT: Technology in Social Context, ed. Ch. Christensen. Cambridge Scholars Press, 2008.

[101] Pfitzmann, B., Waidner, M., & Pfitzmann, A. *Rechtssicherheit trotz Anonymitt in offenen digitalen Systemen.* Datenschutz und Datensicherung DuD, 14/5-6:243-253, 305-315, 1990. translated into English: Secure and Anonymous Electronic Commerce: Providing Legal Certainty in Open Digital Systems Without Compromising Anonymity, IBM Research Report RZ 3232 93278) 05/22/00, IBM Research Division, Zurich,May 2000.

[102] Pfitzmann, A., & Hansen, M. *Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology*. v0.30.pdf, 26 Nov. 2007. http://dud.inf.tu-dresden.de/Anon_Terminology.shtml

[103] Porter M, Millar VE. *How information gives you competitive advantage*. Harvard Business Review Vol 63 Issue 4 Jun/July 1985 pp. 149-160.

[104] PRIME Deliverable D14.2.c, Architecture V2, https://www.prime-project.eu/

[105] PRIME. PRIME Workplan — Description of Work, 2003.

[106] PRIME internal deliverable 'F1'

[107] PRIME internal deliverable 'F2'

[108] Project Management Institute. *A Guide to the Project Management Body of Knowledge*, 2000 ed., 2000.

[109] Proposal for a Directive of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on consumer protection cooperation, pp. 12

[110] Punie, Y. *A social and technological view of ambient intelligence in everyday life: What bends the trend?* The European Media and Technology in Everyday Life Network, 2003.

[111] Raab, C. D. *Governing the safety state*. Tilburg Safety Seminar. Tilburg, 2007.

[112] Rachels, J. *Why privacy is important.* Philosophy and Public Affairs, pp. 323-333, 1975.

[113] Rannenberg, K., *How much negotiation and details can users handle? Experiences with security negotiation and the granularity of access control in communications*. Computer Security - ESORICS 2000, Proceedings of the 6th European symposium on Research in computer Security, Toulouse/France, October 2000

[114] Raskin, J. *The Humane Interface - New Directions for Designing Interactive Systems*. ACM Press, New York, 2000.

[115] Rawashdeh, A. and Matalkah, B. *A New Software Quality Model for Evaluating COTS Components*. Journal of Computer Science 2(4); pp. 373-381, 2006.

[116] Regan, P. M. *Legislating privacy; technology, social values, and public policy*. The University of North Carolina Press, 1995.

[117] Rivera M.A. & Rogers E.M., *Evaluating public sector innovation in networks: extending the reach of the national cancer institute's web bases health communication intervention research initiative*. The Innovation Journal: The public Sector Innovation Journal, 2004/9, pp. 1-5, 2004.

[118] Rogers E.M. *Diffusion of Innovations*, New York: Free Press, 2003.

[119] Rose F., *The economics, concept and design of information intermediaries.* Heidelberg: Physica- Verlag, 1999.

[120] Rotenberg, M., & LaUrant, C. *Privacy & Human Rights. An International Survey of Privacy Laws and Developments.* Tech. rep., EPIC and Privacy International, 2004.

[121] Rotenberg, M. *Real ID, real trouble?* Communications of the ACM, 49(3), pp. 128-128, 2006.

[122] SET Secure Electronic Transaction LLC. The set standard specification, May 1997. originally at http://www.setco.org/set specifications.html; now mirrored at http://www.cl.cam.ac.uk/research/security/resources/SET/.

[123] Slone, S., & The Open Group Identity Management Work Area. *The open group identity management white paper*, March 2004.

[124] Smith, A., & Clarke, R. *Identification, authentication and anonymity in a legal context.* In User Identification & Privacy Protection, S. et al., Eds., IFIP WG 8.5/9.6, June 1999.

[125] Smith, R. *The real jukebox monitoring system.* Computerbytesman.com, 1999.

[126] Solove, D. J *Conceptualizing privacy.* California Law Review, 90, pp.1087-1155, 2002.

[127] Solove, D. J. *Identity theft, privacy, and the architecture of vulnerability*. Hastings Law journal, 54, 2003.

[128] Stalder, F. *The failure of privacy enhancing technologies (PETs) and the voiding of privacy.* Sociological Research Online, 7(2), 2002.

[129] Surveillance Studies Network. A report on the surveillance society: Surveillance Studies Network, 2006.

[130] Schwartz, B. *The social psychology of privacy.* The American Journal of Sociology, 73(6), pp. 741-752, 1968.

[131] Tavani, H. T., & Moor, J. H. *Privacy protection, control of information and privacy-enhancing technologies.* Computers and Society, 2001.

[132] Taylor, C. R. *Private demands and demands for privacy: Dynamic pricing and the market for customer information.* Department of Economics, Duke University, pp. 31, 2002.

[133] Telia FriendFinder, http://trainingcenter.telia.se/articles/00/00/5c/47/01/.

[134] Title V EU Treaty

[135] Title VI EU Treaty

[136] UK Information commissioner, *Guidance to the privacy and electronic communications (EC Directive) Regulations – Part 1: marketing by electronic means, v3.0.* pp. 5, May 2004. available online at http://www.ico.gov.uk/documentUploads/Electronic%20Communications%20Part%201%20Version%203.pdf

[137] vandecasteele J., Moerland L. *Groeimodel voor IV-functie – Het systematisch weergeven van een herinrichtingproces*. KPMG Management Consulting; December 2, 2001

[138] Van Dijk, J., & Hacker, K. *The digital divide as a complex and dynamic phenomenon.* The Information Society, 19, pp. 315-326, 2003.

[139] Volanis, N. *Privacy, piracy and digital rights management: The good, the bad and the ugly?* In Paper presented at the 2nd Greek national conference with international participation: Electronic democracy - challenges of the digital era, Athens, 16-17 March 2006.

[140] Wang, R. Y. *A product perspective on total data quality management.* Communications of the ACM, February 1998.

[141] Ward M. *Sony Slated over Anti-Piracy CD.* BBC News, 2005.

[142] Webster. Merriam webster online dictionary, 2006.

[143] Wellman, B., & Gulia, M. *Net surfers don't ride alone: Virtual communities as communities.* In P. Kollock & M. Smith (Eds.), Communities and cyberspace. New York: Routledge, 1999.

[144] Wellman, B., Quan-Haase, A., Boase, J., & Chen, W. *The social affordances of the internet for networked individualism.* Journal of Computer-Mediated Communication, 8(3), 2003.

[145] Westen, P. *The logic of consent: The diversity and deceptiveness of consent as a defense to criminal conduct.* Aldershot/Burlington: Ashgate, 2004.

[146] Westin, A. *Privacy and freedom*. New York: Atheneum, 1967.

[147] Wilkins, J. *Web 2.0; what does it mean and why does it matter?* Doc Magazine, 21(4), pp. 10-11, 2007.

[148] Woodward, J. D. *Biometrics: Identifying law and policy concerns.* In A. K. Jain, R. Bolle & S. Pankanti (Eds.), Biometrics: Personal identification in networked society, pp. 385-406. Dordrecht: Kluwer Academic, 2002.

[149] World Wide Web Consortium. *P3P protocol specification*. Tech. rep., World Wide Web Consortium, 1998.

[150] World Wide Web Consortium. *The Platform for Privacy Preferences 1.0 (P3P1.0) Specification*, W3C Recommendation 16 April 2002, http://www.w3.org/TR/P3P/

[151] WP 2.1, & WP 2.2. Requirements version 0 (Deliverable): PRIME Consortium, 2005.

[152] WP 4.2. Evaluation of final application prototypes (Deliverable): PRIME Consortium, 2008.

[153] Zaltman G., et al. *Innovations and organizations*, New York: John Wiley & Sons Inc, 1973.

[154] Ziller, Jacques, *The Prüm Convention: A Real-False Reinforced Cooperation in the Area of Freedom, Security and Justice of the EU and EC Treaties (Le Traité de Prüm une Vraie-Fausse Coopération Renforcée dans L'Espace de Sécurité de Liberté et de Justice)*. December 2006. Available at SSRN: http://ssrn.com/abstract=965714

Appendix A Summary of privacy process design measures and their relation to legal and social requirements

Common socio-legal requirements		**Service Provider Response to socio-legal requirements**	
Legal Requirement	**Social requirement**	**Addressed by Organizational Measures**	**Addressed by Technical Measures**
Information to the user/ Transparency (see section 5.2.2.1)			
The following minimum information has to be provided to the data subject: the identity of the controller or her representative, the purposes of the processing for which the data are intended, any further information if this is necessary to guarantee fair processing in respect of the data subject, such as the recipients or categories of recipients of the data, whether replies to the questions are obligatory or voluntary, as well as the possible consequences of the failure to reply and the existence of the right of access to and the right to rectify the data concerning her. (Art. 10 data protection directive) Exceptions are foreseen in Art. 11(2) data protection directive mainly for statistical purposes or for the purposes of historical or scientific research.	Disclosure of information to a user is a prerequisite for individual control over personal information. Next to the legal obligations for dissemination of information, information needs to contribute to consciousness of the user about collection of data. Furthermore, information should be provided in a comprehensible format and should provide the user a 'glimpse into the future', by showing the consistency of the procedure of data processing. In addition, the provision of information is a useful instrument to effectuate trust in a data transaction partner.	Organizations can take the following organizational or policy measures to address these needs: Publication of nature of data registration, purposes, data controller, any automatic decision-making & privacy policy for data subjects Data Model & data flows Privacy Risk Assessment Privacy audit/seal	Organizations can ask for the necessary technical measures to address these needs: Is there an automatic interface/link between the central logbook/listing of personal data processing and the registrations/databases itself? Is there an interface/link between the internal listing and the listing submitted to the data protection authority? Is the data subject automatically provided with information on the type and nature of the processing of her personal data?

Consent of the user (see section 5.2.2.2)			
Consent is defined as any "freely given specific and informed indication of her wishes by which the data subject signifies her agreement to personal data relating to her being processed" (Art. 2(h) data protection directive).	Consent of a user needs to imply that the user has got an actual choice whether or not to engage in a service. In other words: a 'take-it-or-leave-it' approach still forces the disclosure of personal information and is unwanted. In addition, the user needs to be able to confine the use of her personal information, by determining the specific boundaries in which data can be processed.	Organizations can take the following organizational or policy measures to address these needs: Obtaining signed consent form (incl. Verification of identity) Obtaining opt-in for direct marketing e-mails (otherwise it's spam)	Organizations can ask for the necessary technical measures to address these needs: Is the contact data of each data subject recorded, including when a legal representative is required? Is the unambiguous consent or other grounds for processing inseparably linked to the data obtained itself? Is the opt-in or opt-out being enforced automatically? Are special categories of personal data (religion, race, political opinions, health, sex life, trade union membership, etc.) in the database labeled/tagged for specific way of (automatic) processing?
Users' right to access the data (see section 5.2.2.3)			
Every individual has the right to obtain from the data controller: confirmation as to whether or not her personal data are being processed and information at least as to the purposes of the processing, the categories of the data concerned, and the recipients or categories of recipients to whom the data are disclosed, communication to her in an intelligent form of the data undergoing processing and of any available information to	For a user to have control over personal information, subjects need to be able to inspect the effects of the application of their data. This implies access to data. Access to data and the possibility of inspection are a countervailing power in the imbalanced relation between data subject and data controller. It needs to be noted that this possibility for inspection should be carried out	Organizations can take the following organizational or policy measures to address these needs: Publication of nature of data registration, purposes, data controller, any automatic decision-making & privacy policy for data subjects Privacy audit/seal	Organizations can ask for the necessary technical measures to address these needs: Is the data subject automatically provided with information on the type and nature of the processing of her personal data? Is this also applicable when the data is obtained from a third party (rather than from the data subject itself)? Is there an electronic means for data subjects to object against the processing of her data

the resources and of any available information as to their source. (Art. 12(a) data protection directive) Where any automated decisions are involved, the data subject has the additional right to be informed about the logic involved in any automatic processing of data concerning her (Art. 15 data protection directive)	throughout the service chain, meaning all the relevant actions considering personal data of the several partners in a service.		(automatically applied in registration/ processing)? Is the information system implemented auditable?
Rectification, erasure, and blocking of data and the right to object (see section 5.2.2.4)			
The data subject has the right to rectify, erase or block the data, the processing of which does not comply with the provisions of the data protection directive, in particular because of the incomplete or inaccurate nature of the data. (Art. 12 (b) data protection directive) The data subject has the right to object to the processing of her personal data, mainly in cases of direct marketing (Art. 14 data protection directive)	Mistakes, unlawful behaviour, and regret need to be possible to redress, as sometimes the disadvantages of dissemination of personal information are only visible with hindsight. In some occasions, rectification, erasure, and blocking of data are important to provide the user a 'fresh start', or a 'second chance'.	Organizations can take the following organizational or policy measures to address these needs: Appoint point of contact for requests & complaints-handling Procedure for right to object to certain data processing & automatic decision-making Procedure for manual follow-up after automatic decision-making	Organizations can ask for the necessary technical measures to address these needs: Is being recorded which data is provided when to which person or which third party? Are corrections requested by the data subject automatically processed in all personal data registrations, incl. in offline and backup data? Is the information system able to provide the logic about automatic decision-making in a transparent way? Is a 'data blockade' (when a data subject has objections against sharing or storing data) being stored with the applicable personal data and is it automatically enforced? Is data deletion/destruction being logged in a secure way? Are the legal

			representatives of data subjects under the age of 16 being stored with the applicable personal data?
Data security (see section 5.2.2.5)			
Data controllers shall take 'appropriate technical and organizational measures' against unauthorised or unlawful processing, and accidental loss, destruction or damage to the data (Art. 17 (1) data protection directive)	Data is security is of importance, to ensure the user that data cannot flow outside the determined boundaries for use of information. Furthermore, a secure infrastructure can contribute to trustworthiness. The provided information considering security measures, however, needs to be tailored to the context of the user, meaning a broad use of understandable markers about the used infrastructure *and* the about the partners one engages with.	Organizations can take the following organizational or policy measures to address these needs: Security Policy (incl. risk assessment) Data Classification Personnel Security, Screening & Non-Disclosure Agreement Security Awareness Segregation of Duties Physical & Logical Identity & Access Management procedures Change, Problem/Incident & Configuration Management procedures Contingency Plan (incl. Training & Testing) Security Monitoring & Auditing (incl. appointing internal or external auditor)	Organizations can ask for the necessary technical measures to address these needs: Is strong authentication (i.e. token, biometric, digital certificates) being applied to gain access to the information system? Can personal data be divided in multiple data domains, each with its own security regime? Can the data domains only be combined by authorised staff (and not by IT staff)? Is role-based and/or attribute-based access controls in place to protect personal data? Can temporary access rights be applied? Are security measures be dependent on the risk classification of the data items/fields involved? Is that risk classification even stored with the applicable data? Is automatic logout and screensaver with some kind of protection being applied? Are all relevant IT infrastructure and physical security measures being implemented? Are successful as well as unsuccessful, authorised as well as

			unauthorised access attempts being logged? Can access to specific personal data (domains) be blocked automatically? Is personal data (incl. traffic header and location data) exchanged over public networks in an encrypted manner? Is sensitive personal data being stored in an encrypted or other secure manner? Is all personal data periodically being stored for recovery purposes? Are all relevant security measures also applicable to backup data?
Legal Data Protection Principles		**Service Provider Response to these legal requirements**	
		Addressed by Organisational Measures	**Addressed by Technical Measures**
Purpose limitation and Data minimisation (see section 5.2.1)			
The finality or purpose limitation principle provides that data controllers must collect data only as far as it is necessary in order to achieve the specified and legitimate purpose they pursue, and cannot carry out any further processing which is incompatible with those purposes (Art. 6(1)(b) data protection directive). According to data minimisation principle the processing of personal data should be limited to data that are adequate, relevant and not excessive. Consequently, data controllers are obliged to store only a minimum of data sufficient to run their services (Art. 6(1) (d) data protection directive)		Organizations can take the following organizational or policy measures to address these needs: Privacy Impact Assessment (for all – current & future – types of processing) Software development approach contains data minimisation	Organizations can ask for the necessary technical measures to address these needs: Is the purpose for processing inseparably linked to the data itself? Is data minimisation achieved in the data model? Are there technology measures in place so that personal data cannot be retained longer than necessary (from a data processing objective perspective)?

Principle of Restricted Data Transfer to Third countries (see section 5.2.1)		
The transfer of personal data to countries outside the European Union is in principle only permitted if the third country in question ensures an adequate level of protection (Art. 25 data protection directive).	Organizations can take the following organizational or policy measures to address these needs: Listing of adequate protection countries	Organizations can ask for the necessary technical measures to address these needs: Is there an automatic check if data is transferred to EU or other eligible third country (according to Art. 26 data protection directive)?